Australian Human Rights Commission

Review of the *Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018* (Cth)

Submission to the Independent National Security Legislation Monitor

20 September 2019

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

Australian Human Rights Commission
www.humanrights.gov.au

Table of contents

1 Introduction

1. The Australian Human Rights Commission (the Commission) welcomes the opportunity to make this submission to the Independent National Security Legislation Monitor (INSLM) review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (the TOLA Act), and, in particular, whether that Act:

    i. contains appropriate safeguards for protecting the rights of individuals
    ii. remains proportionate to any threat of terrorism or threat to national security, or both
    iii. remains necessary.

2. The TOLA Act introduced new powers for certain law enforcement, security and intelligence agencies to access electronic information that would previously have remained private. For example, certain agencies are empowered to compel the decryption of text messages, compel access to electronically protected files, or require a person to unlock their phone.

3. Such measures can significantly limit a person's rights to privacy, freedom of expression and freedom from arbitrary detention among other human rights. The stated aim of the reforms is to 'introduce measures to better deal with the challenges posed by ubiquitous encryption'.[1] The limits on human rights have been claimed to be justified on the basis of a need to combat serious crime and to protect public safety.[2]

4. The Commission acknowledges these important and legitimate goals. However, under international human rights law, Australia's law enforcement powers must be precisely targeted to restrict human rights no more than is absolutely necessary to achieve these legitimate aims. The Commission considers that the TOLA Act does not meet this international law requirement.

5. Rather, the TOLA Act permits inappropriately intrusive, covert and coercive powers, without effective safeguards to adequately protect relevant human rights. The consequent limitations on human rights are potentially far-reaching. Most obviously, the TOLA Act restricts the rights of people under investigation by law enforcement or intelligence agencies. However, the TOLA Act extends also to limit the rights of a vast number of other users of technology—the overwhelming majority of whom will be innocent

third parties who are not suspected of any wrongdoing. On the basis of publicly available information, the Commission considers that many of the TOLA Act's limitations on human rights have not been shown to be reasonable, necessary and proportionate.

6. The Commission notes that this review occurs in the context of recent inquiries conducted by the Department of Home Affairs (the Department) and the Parliamentary Joint Committee on Intelligence and Security (the Committee) into this legislation. The INSLM review is the result of a reference from the Committee, to inform its ongoing review into the TOLA Act.

7. The Commission has actively engaged in these reviews to inform the development of this legislation to date, making three detailed submissions. On 10 September 2018, the Commission made a detailed submission to the Department of Home Affairs on an exposure draft of the TOLA Bill (the draft TOLA Bill). On 12 October 2018, the Commission made a further detailed submission to the Committee on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the TOLA Bill). On 22 February 2019, the Commission made a submission to the Committee on the TOLA Act as passed.

8. The short timeframes for consultation on the complex and substantial iterations of these reforms, and the passage of the Act on 6 December 2018—which included Government amendments introduced over the course of that day (the Government amendments)—has made meaningful parliamentary and public scrutiny challenging.

9. The Commission and members of the public are also not privy to any classified information that may be provided to the INSLM by Government departments and agencies to inform his review. The Commission would welcome any further information that could be publicly released by the INSLM and relevant agencies about the claimed need for, and the use and operation of, the scheme to date in advance of the INSLM's public hearings. Such information could usefully include, for example, information about the number of times the assistance scheme has been used, for what types of relevant objectives, and the instances in which the new or expanded other powers enacted by Sch 2-5 of the TOLA Act have been used. To the extent possible, it would be useful also to release an unclassified summary of the evidence said to support the claimed need for the provisions. This would allow the Commission and other submitters to make more informed comment.

10. Such scrutiny is vital in the case of legislation that significantly curtails human rights, to ensure that such laws are passed only where they are clearly needed, and that they are carefully tailored to ensure they do not encroach on human rights any more than is necessary.

11. The TOLA Act as passed is, in many respects, substantially similar to the TOLA Bill. A relatively small number of changes were made to the TOLA Bill by way of the Government amendments. Some of the amendments implemented some of the Commission's previous recommendations. However, reading the TOLA Act as a whole, the Commission retains serious concerns about the Act's human rights impact.

12. The Commission reiterates the 54 recommendations made in its previous submission on the TOLA Bill dated 12 October 2018 (the Commission's October 2018 submission), many of which continue to apply to the TOLA Act as passed. This submission is **annexed** for consideration by the INSLM.

13. The Commission's primary recommendation is that the 54 recommendations made in its submission on the TOLA Bill be implemented in full. It does not repeat the substance of that submission or each recommendation here.

14. Rather, this submission focuses on five particularly significant ongoing concerns about inadequate human rights safeguards in the TOLA Act. It does not exhaustively address all of the remaining human rights issues.

2 Summary

15. Schedule 1 of the TOLA Act created an assistance and access scheme that empowers certain agencies to request or compel a 'designated communications provider' to provide them with technical assistance.[3]

16. Schedules 2–5 of the TOLA Act significantly broadened the evidence-gathering powers available to law enforcement and security agencies to access electronic information, for example by way of a new 'computer access warrant' regime in the *Surveillance Devices Act 2004* (Cth) (SD Act). These schedules also amended nine pieces of existing Commonwealth legislation, including the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act), to enhance investigative powers.

17. Overall, the TOLA Act created broad new powers to enable government agencies to gain access to information that would otherwise remain private—for example, by virtue of encryption.[4]

18. The Commission holds serious concerns that the significantly enhanced abilities of agencies to gather and access electronic information limits human rights in a manner that is not a necessary and proportionate response to legitimate objectives.

19. In summary, the five key concerns highlighted in this submission are:

    i. the lack of a requirement for judicial authorisation for the giving of Technical Assistance Notices and Technical Capability Notices
    ii. the ambiguity of the 'systemic weakness' and 'systemic vulnerability' limitations, which seek to prohibit some of the 'acts or things' that can be requested or compelled under the assistance scheme
    iii. the breadth of 'relevant objectives' for which the assistance scheme may be used
    iv. the breadth of the Australian Security Intelligence Organisation's mandatory assistance powers introduced by Schedule 5 of the TOLA Act
    v. the breadth of the 'concealment of access' powers introduced by Schedules 2 and 5 of the TOLA Act.

20. The recommendations made with respect to these five issues (set out below) would partly address some of the more serious rights interferences permitted by the TOLA Act, but would far from fully address all of the concerns identified in the Commission's October 2018 submission.

21. The Commission supports further review and reform of the TOLA Act consistent with its October 2018 submission, and full implementation of all 54 recommendations contained in that submission. As noted above, while a small number of these recommendations were addressed through Government amendments to the TOLA Bill, the vast majority of the Commission's previous recommendations still need to be addressed. However, at this juncture, the Commission urges the INSLM:

    i. to scrutinise closely the claims that the measures in the TOLA Act are necessary and proportionate, in light of the significant human rights limitations identified in this submission

ii. to recommend that the Government implement all of the Commission's outstanding recommendations, prioritising those referred to below.

3 Recommendations

22. With respect to the five issues set out in this submission, the Commission makes the following recommendations:

Recommendation A

Recommendations 14, 28, 30 and 31 in the Commission's October 2018 submission should be implemented in full, in particular that judicial authorisation be required for the giving or varying of notices under the assistance scheme.

Recommendation B

In the event that Recommendation A is not implemented, s 317WA of the *Telecommunications Act 1997* (Cth) should be amended to make the report of assessors regarding a proposed Technical Capability Notice binding on the Attorney-General.

Recommendation C

An independent assessment process commensurate to that contained in s 317WA of the *Telecommunications Act 1997* (Cth), or some other appropriate and similar form of independent review, should be made available with respect to Technical Assistance Requests and Technical Assistance Notices, not just Technical Capability Notices.

Recommendation D

The Government consult widely with industry and technical experts, as well as bodies with human rights expertise, to formulate and implement a revised 'systemic weakness' limitation in s 317ZG of the *Telecommunications Act 1997* (Cth) that is clear, precise, and prohibits action that would detrimentally affect the cybersecurity and privacy of a significant proportion or number of innocent third parties, or that would weaken a significant part or whole of a relevant system.

Recommendation E

If Recommendation D is not accepted, the Government seek and publish legal advice as to the interaction between ss 317B and 317ZG of the *Telecommunications Act 1997* (Cth), and implement reforms to ensure that

an 'act or thing' cannot be requested or compelled under the assistance scheme if it would jeopardise or be likely to jeopardise the information security of innocent third parties.

Recommendation F

The 'relevant objectives' for which Technical Assistance Requests may be issued should be further amended so that it is not possible to use the assistance scheme for purposes related to 'the interests of Australia's national economic well-being', and so that the meaning of 'matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means' is more clearly and precisely defined.

Recommendation G

The definition of 'serious offence' in s 317B of the *Telecommunications Act 1997* (Cth) should be amended so that it is consistent with the definition in s 5D of the *Telecommunications (Interception and Access) Act 1979* (Cth).

Recommendation H

Section 34AAA of the *Australian Security Intelligence Organisation Act 1979* (Cth) should be amended to include protections for persons compelled to attend or remain in a specified place under an assistance order, in line with Recommendation 48 of the Commission's October 2018 submission.

Recommendation I

The *Australian Security Intelligence Organisation Act 1979* (Cth) and the *Surveillance Devices Act 2004* (Cth) should be amended so that, if it is not reasonably practicable for 'concealment of access' to occur while a warrant is in effect, or within 28 days of its expiry, law enforcement authorities are required to return to an eligible Judge or nominated Administrative Appeals Tribunal member or, in the case of Australian Security Intelligence Organisation warrants, the Attorney-General for further authorisation before any of the concealment of access powers introduced by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) can be exercised.

4 Human rights and digital law enforcement

23. The human rights to privacy and freedom of opinion and expression are protected under articles 17 and 19 of the *International Covenant on Civil and Political Rights* (ICCPR).[5]

24. These rights are related and mutually reinforcing—for instance, an individual's privacy facilitates their freedom of expression.[6] They are also an essential precondition for the proper protection of *all* human rights,[7] as well as the robust and representative nature of Australian democracy.

25. As a party to the ICCPR and other relevant international human rights treaties,[8] 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.

26. The rights to freedom of expression and freedom of opinion have been described by the United Nations Human Rights Committee (UN 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'.[9]

27. The increasing use of digital technology for surveillance and related purposes, by police and other law enforcement bodies, poses new challenges to the protection of human rights, such as the rights to privacy and freedom of expression. The TOLA Act helps facilitate digital surveillance and interception of communications by certain government agencies. In particular, through supporting the decryption of digital communications, certain agencies are now able to understand and read information in a digital format collected through surveillance or interception, in circumstances where this information otherwise would have been likely to remain private.

28. 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.[10]

29. 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.[11] 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.[12]

30. The UN Office of the High Commissioner for Human Rights (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.[13]

31. 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.[14]

4.1 Right to privacy

32. 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.

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

34. The right to privacy is especially important in the context of the TOLA Act, 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).

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

36. '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.[15]

37. 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.[16]

38. 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.[17]

39. The 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.[18]

4.2 Right to freedom of expression

40. 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.

41. 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'.[19] It also protects the freedom to seek, receive and impart information and ideas of all kinds, free from unlawful interference.

42. 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'.[20] It is also necessary for the effective exercise of the right to vote.[21]

43. 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.[22]

4.3 Other human rights

44. Other human rights may also be inappropriately limited by the unnecessary or disproportionate exercise of digital surveillance, interception and decryption by law enforcement agencies. These include a person's enjoyment of their rights to freedom of religion, a fair hearing and equality.[23]

45. 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[24] and persons engaging in lawful public dissent. Children's rights may also be affected by the use of 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.[25]

46. Given the potentially significant and far-reaching consequences of digital law enforcement powers on human rights, it is crucial to ensure that any rights limitations they impose 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.

4.4 Permissible limitations on human rights

47. 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.[26]

48. 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.

49. There is some overlap between a number of these criteria.[27] 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'.[28]

(a) Legitimate aims

50. 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.

51. 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.[29]

52. 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 exist adequate safeguards and effective remedies against abuse.[30] 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. [31]

(b) Necessity

53. 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 available methods of gathering evidence.

54. 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.[32]

55. 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.

56. 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.[33]

57. 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.[34]

58. To establish necessity, the powers must be closely scrutinised to determine whether they go beyond what is genuinely needed for the purposes of law enforcement.

(c) Proportionality

59. The Siracusa Principles state that a rights limitation must pursue a legitimate aim and be proportionate to that aim.[35] 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.

60. 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.[36]

61. 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.[37]

62. A fully informed assessment of these issues may, in some circumstances, depend on the consideration of classified security material. Often, only the relevant decision makers empowered to give notices or to obtain warrants will have access to this information, which is not made publicly available. Therefore, it is difficult to scrutinise these decisions and ensure that human rights are protected. In the Commission's view, it is accordingly crucial that human rights protections are built into the decision-making process, as a safeguard to support proper consideration of human rights by decision makers in all the relevant circumstances.

5 Five key human rights concerns

Schedule 1 of the TOLA Act

5.1 Lack of a requirement for judicial authorisation for assistance notices

63. The TOLA Act introduced new powers under which designated communications providers can be compelled to provide certain government agencies with various forms of technical assistance.

64. As explained in the Commission's October 2018 submission on the TOLA Bill, the Commission considers that:

    a) agencies should not be able to compel technical assistance without first obtaining independent judicial authorisation (see Recommendation 28 of the Commission's October 2018 submission)

    b) providers who receive notices compelling them to provide technical assistance should have access to independent merits review of decisions made under Pt 15 of the *Telecommunications Act 1997* (Cth) (the Telecommunications Act), including of a decision to give a notice (see Recommendations 14 and 31 of the Commission's October 2018 submission)

    c) providers should have access to judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) (see Recommendation 30 of the Commission's October 2018 submission).

65. The Government amendments to the TOLA Bill introduced an assessment process in s 317WA of the Telecommunications Act, allowing affected providers to request an assessment of whether a proposed Technical Capability Notice (TCN) should be given.

66. However, there is still no requirement that judicial authorisation be obtained before a TCN or a Technical Assistance Notice (TAN) is given. This process does not ensure robust, independent and transparent decision making in relation to the giving of notices. The Commission repeats Recommendations 14, 28, 30 and 31 made in its October 2018 submission, for the reasons given in that submission.

67. If, contrary to the recommendations made in the Commission's October 2018 submission, a requirement for judicial authorisation is not

introduced, the effectiveness of s 317WA could be enhanced by making the outcome of the assessment process binding. A commensurate assessment process should also apply to TANs and Technical Assistance Requests (TAR), as well as TCNs.

68. As noted above, s 317WA allows the recipient of a proposed TCN to request an assessment of whether the notice should be given. Following such a request, the provision currently allows for two assessors, being a person with relevant technical expertise and a former judge, to consider whether the building of the new capability would contravene the 'systemic weakness' limitation and/or the 'systemic vulnerability' limitation in s 317ZG (hereafter referred to as the 'systemic weakness' limitation).[38]

69. Under s 317W(7), the assessors must also consider whether the requirements imposed by the proposed TCN are reasonable and proportionate, whether compliance is practicable and technically feasible, and whether it is the least intrusive measure that would be effective in achieving the legitimate objective of the proposed notice. Under s 317WA(11), the Attorney-General must 'have regard' to the resulting report of the assessors. That is, the decision of the assessors is *not binding* and could ultimately be ignored.

70. The Commission considers that a non-binding form of assessment severely diminishes the integrity of the process and the utility of engaging experts with technical knowledge and a degree of independence to review proposed TCNs.[39]

71. Further, the assessment process currently only applies to TCNs and not to other forms of technical assistance. TANs and TARs are also potentially onerous on those who receive them, and rights-intrusive for third parties. They could also potentially be given (or purportedly given) in any or all of the following circumstances:

    a) where the request is not reasonable and proportionate
    b) where compliance with the request is not practicable and technically feasible
    c) where they would not be the least intrusive form of assistance
    d) where other relevant requirements of the Telecommunications Act are not met.

72. The Commission considers that TARs and TANs should be subject to either a similar assessment process to that established in s 317WA or some other appropriate form of independent review.

73. The Commission notes a further change made to the TOLA Bill before passage that altered the oversight of the TCN regime. Section 317TAAA(1) of the Telecommunications Act requires the Minister for Communications and the Arts to approve the giving of a TCN, in addition to the Attorney-General. However, as these are both ministerial approvals, the Commission considers that this additional approval does little to enhance the independence of decision making, especially as compared with the preferred scenario of independent judicial authorisation.

74. The Commission notes the amendments proposed in Sheet 8627 to the TOLA Bill by Senator the Hon Penny Wong on 6 December 2018, providing that an eligible judge must approve the giving or variation of a TAN or TCN, after being satisfied of certain matters on the basis of evidence. The Senate did not agree to that proposed amendment. It does not form part of the TOLA Act. However, the Commission considers that the proposal would better address its human rights concerns, as compared to the current oversight of the assistance scheme.

Recommendation A

Recommendations 14, 28, 30 and 31 in the Commission's October 2018 submission should be implemented in full, in particular that judicial authorisation be required for the giving or varying of notices under the assistance scheme.

Recommendation B

In the event that Recommendation A is not implemented, s 317WA of the *Telecommunications Act 1997* (Cth) should be amended to make the report of assessors regarding a proposed Technical Capability Notice binding on the Attorney-General.

Recommendation C

An independent assessment process commensurate to that contained in s 317WA of the *Telecommunications Act 1997* (Cth), or some other appropriate and similar form of independent review, should be made

available with respect to Technical Assistance Requests and Technical Assistance Notices, not just Technical Capability Notices.

5.2 'Systemic weakness' limitation remains ambiguous

75. A TAR, TAN or TCN must not require a provider to do something that would introduce a 'systemic vulnerability' or 'systemic weakness' into a form of electronic protection. Those terms were not fully defined in the TOLA Bill as first introduced. The Commission recommended that these terms be precisely and clearly defined (see Recommendation 15 of the Commission's October 2018 submission).

76. The Government amendments made to the TOLA Bill before its passage introduced relevant definitions. Section 317B of the Telecommunications Act currently provides:

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

77. Section 317B of the Telecommunications Act also defines 'target technology'. Under that definition, a particular carriage service, electronic service, software or software update on a computer or item of equipment, an item of customer equipment or a data processing device that is used or likely to be used by a particular person is 'target technology' connected with a person. It is immaterial whether the person can be identified. 'Electronic protection' is also defined, to include authentication and encryption.

78. Subsection 317ZG(1) of the Telecommunications Act sets out the prohibition on a TAR, TAN or TCN requiring a provider to implement or build a systemic weakness or vulnerability into a form of electronic protection, or from rectifying a systemic weakness or vulnerability.[40] A request or notice will have no effect to the extent that it contravenes s 317ZG(1).

79. Subsections 317ZG(4A)–(4C) were introduced by the Government amendments to the TOLA Bill prior to its passage, and provide:

> (4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.
>
> (4B) In a case where a vulnerability is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic vulnerability into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.
>
> (4C) For the purposes of subsections (4A) and (4B), an act or thing will, or is likely to, jeopardise the security of information if the act or thing creates a material risk that otherwise secure information can be accessed by an unauthorised third party.

80. These provisions purport to govern situations where a weakness or vulnerability is selectively introduced into a target technology. It appears that they were intended to introduce a safeguard, to prevent action that would 'jeopardise' the security of information of people who are not the direct targets of a request or notice.

81. The Supplementary Explanatory Memorandum to the Bill describes the purpose and operation of the safeguard as follows:

> This definition makes clear that a systemic weakness is something that makes general items of technology less secure. Technological classes include particular mobile device models carriage services, electronic services or software. The term is intended to encompass both old and new technology or a subclass within a broader class of technology; for example an iOS mobile operating system within a particular class, or classes, of mobile devices. Where requirements in a notice make the whole set of these items more vulnerable, it will be prohibited. This ensures that the powers do not jeopardise the general use of technology by persons who are not of interest to law enforcement and security agencies. The intent of the prohibition as expressed in the definition is to rule out requirements that would create a material risk of otherwise secure information being accessed by unauthorised third parties.

82. The Commission supports the aim of restricting the scope of the industry assistance provisions, to ensure they cannot be used in ways that make the information of people who are not of interest to relevant agencies less secure. For instance, the powers should not permit the introduction of a weakness into all devices of a particular kind, which could be exploited by unauthorised third parties.

83. The Commission also supports restricting the use of the industry assistance provisions to ensure that relevant agencies can only use the scheme in relation to individuals who are legitimately of interest to them, and in a proportionate manner. That is, the provisions should not allow agencies to require providers to develop tools that give them the ability to access all encrypted communications of a particular kind, including those passing between people not suspected of wrongdoing, or where communications are not reasonably connected to a particular and legitimate matter.

84. However, the Commission considers that the current form of the 'systemic weakness' limitation: is ambiguous; is potentially internally incoherent; permits extensive access to information beyond what is necessary in a particular instance; and could result in the harms that it intends to protect against.

85. First, the meaning of a 'class of technology' in the definitions of systemic weakness and systemic vulnerability is not clear. This term is not legislatively defined. The Supplementary Explanatory Memorandum states that a 'class' includes 'particular mobile device models, carriage services, electronic services or software'. It further states that the term is intended to encompass both old and new technology or a 'subclass' within a broader class of technology, for example 'an iOS mobile operating system within a particular class, or classes, of mobile devices'. The Commission considers that it is not clear how the boundaries of a class can be drawn, including how small or large a class might be.

86. It appears that a very wide category of technological devices, services or software could be said to constitute a 'class'. For example, 'devices allowing electronic communication' could meet the definition of a 'class', and is evidently extremely broad so as to serve no protective function. The Commission queries how useful the concept of a 'class' is. If this concept is maintained, it should be clearly and precisely defined to protect the privacy and cybersecurity of innocent third parties.

87. Second, the requirement that a systemic weakness or vulnerability affect a '*whole* class of technology' is an overly high bar. The word 'whole' implies that the *entire* relevant category of device or service or software must be affected before a systemic weakness is established. The Supplementary Explanatory Memorandum states that 'where requirements in a notice make the whole set of these items more vulnerable, it will be prohibited'.

88. The Commission is concerned that there may be circumstances where, for example, a measure has detrimental impacts on a significant proportion of users, or a significant number of users, but not all users, and therefore cannot be said to affect a 'whole' class. It is also unclear, on the natural and ordinary meaning of 'whole' and 'class', how an individual software application could be said to constitute a whole class of technology. For example, the Facebook Messenger phone application is 'software', but it is not evident how it could form a 'class' let alone a 'whole set' of 'items'. The Commission considers that meaning of 'affects a whole class of technology' should be clarified to ensure that the systemic weakness limitation is applied to individual software applications.

89. The Commission considers that s 317G should be amended to prevent assistance measures that have a negative impact on the privacy or cybersecurity of a significant proportion or number of innocent third parties. This should be in addition to prohibiting the weakening of a significant part of a relevant system, as well as the whole system.

90. Third, the Commission is concerned that the interaction between the relevant definitions in s 317B and the limitation in ss 317ZG(4A)–(4C) is not clear, undermining the safeguard that prevents the information security of third parties being jeopardised when a weakness or vulnerability is 'selectively introduced to one or more target technologies'.

91. On one reading, ss 317ZG(4A)–(4C) could overcome the problems identified above, to prevent a weakness being introduced into a target device where it jeopardises the information held by any other person.

92. However, a possible alternative reading of ss 317ZG(4A)–(4C) would give those provisions no effect, as explained below.

93. Section 317B defines 'systemic weakness' to exclude 'a weakness that is selectively introduced to one or more target technologies that are connected with a particular person' from the definition of 'systemic weakness'.

94. Subsection 317ZG(4A) then seeks to reintroduce the scenario of a selectively introduced weakness, into the definition of 'systemic weakness' in ss 317ZG(1)(a)–(b). It provides that a 'systemic weakness' includes 'any act or thing that will, or is likely to, jeopardise the security of any information held by any other person'. Subsection 317ZG(4B) introduces a similar reintroduction for the definition of 'systemic vulnerability', with respect to ss 317ZG(1)(a)–(b).

95. Subsection 317ZG(4C) provides that an 'act or thing' will, or is likely to, 'jeopardise' security of information if it creates a material risk that otherwise secure information can be accessed by an unauthorised third party. The meaning of unauthorised third party is not defined.

96. The Commission considers that, on one reading, these provisions could operate so that s 317B excludes the selective weakness and vulnerability scenarios in ss 317ZG(4A)–(4C) from the definition of 'systemic weakness' and 'systemic vulnerability' that is picked up in ss 317ZG(1)(a)–(b). That would result in the ss 317ZG(4A)–(4C) safeguards having no effect.

97. The Commission considers that the interaction between ss 317B and 317ZG should be clarified, to avoid any doubt and ensure that ss 317ZG(4A)–(4C) operate effectively to prevent the security of any information held by any other persons being jeopardised.

98. The Commission notes the amendments to the Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 (Cth) moved by Senator the Hon Jenny McAllister in Sheet 8642 on 14 February 2019, setting out an alternate form of the 'systemic weakness' limitation in s 317ZG. The formerly constituted Senate agreed to that amendment, but the Bill lapsed with the proroguing of the 45th Parliament.

99. The Sheet 8642 amendment sought to remove ambiguity about the interaction between ss 317B and 317ZG(4A)–(4C), and appears to address several of the Commission's concerns.

Recommendation D

The Government consult widely with industry and technical experts, as well as bodies with human rights expertise, to formulate and implement a revised 'systemic weakness' limitation in s 317ZG of the *Telecommunications Act 1997* (Cth) that is clear, precise, and prohibits action that would detrimentally affect the cybersecurity and privacy of a

significant proportion or number of innocent third parties, or that would weaken a significant part or whole of a relevant system.

Recommendation E

If Recommendation D is not accepted, the Government seek and publish legal advice as to the interaction between ss 317B and 317ZG of the *Telecommunications Act 1997* (Cth), and implement reforms to ensure that an 'act or thing' cannot be requested or compelled under the assistance scheme if it would jeopardise or be likely to jeopardise the information security of innocent third parties.

5.3 'Relevant objectives' too broad

100. Amendments to the TOLA Bill before its passage narrowed the 'relevant objectives' for which TARs, TANs and TCNs may be issued. Despite those changes, the Commission considers that problems remain with the unjustifiably wide breadth of the permitted 'relevant objectives', especially for TARs.

101. The 'relevant objectives' set out in s 317G(5) of the Telecommunications Act permit the giving of a TAR to assist the Australian Secret Intelligence Service in relation to 'the interests of Australia's national economic well-being'. TARs can also be given to assist the Australian Signals Directorate 'on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means'. The Supplementary Explanatory Memorandum does not address the meaning of the latter phrase.

102. The Commission considers that the scope of these objectives is not clear. While measures that significantly limit human rights may, in some circumstances, be permissible to protect national security, it is more difficult to establish proportionality with respect to achieving comparatively less important and pressing objectives. In particular, the concept of 'national economic well-being' could permit use of the assistance scheme for tax and superannuation law compliance.

103. In certain cases, the powers introduced by Schedule 1 of the TOLA Act limit the objectives for which assistance can be compelled or requested to enforcing the criminal law 'so far as it relates to serious Australian offences'. This is a new reform introduced by the Government amendments, that partially implements Recommendation 6 of the Commission's October 2018 submission, to confine the scheme to the

enforcement of serious offences. However, the Commission considers that this reform does not provide for a high enough bar in respect of criminal conduct.

104. 'Serious Australian offence' is defined in s 317B of the Telecommunications Act to mean an offence against a law of the Commonwealth, a State or a Territory that is punishable by a maximum term of imprisonment of 3 years or more, or life.

105. The Commission previously recommended a higher threshold for a serious offence, by reference to s 5D of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) (see Recommendation 6 of the Commission's October 2018 submission). That provision includes offences punishable by imprisonment for life, or a period of at least seven years.

106. The Commission considers that, to establish an appropriately serious threshold of conduct and to ensure legislative consistency, the threshold in s 5D of the TIA Act for a 'serious offence' is a more appropriate minimum bar.

107. The Commission otherwise welcomes the narrowing of 'relevant objectives' that authorise the giving of a request or notice. In particular, it supports the removal of the enforcement of pecuniary penalties as a relevant objective, which enhances the proportionality of the scheme overall.

Recommendation F

The 'relevant objectives' for which Technical Assistance Requests may be issued should be further amended so that it is not possible to use the assistance scheme for purposes related to 'the interests of Australia's national economic well-being', and so that the meaning of 'matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means' is more clearly and precisely defined.

Recommendation G

The definition of 'serious offence' in s 317B of the *Telecommunications Act 1997* (Cth) should be amended so that it is consistent with the definition in s 5D of the *Telecommunications (Interception and Access) Act 1979* (Cth).

Schedules 2–5 of the TOLA Act

108. In its October 2018 submission, the Commission raised serious concerns about the human rights implications of Schedules 2–5 of the TOLA Bill. These issues have received comparatively less public attention than those arising from Schedule 1 of that Act, but are of comparable importance.

109. Schedules 2–5 significantly broaden the intrusive and coercive powers available to law enforcement and security agencies, for example, by way of a new 'computer access warrant' regime in the *Surveillance Devices Act 2004* (Cth) (SD Act). Schedules 2–5 also amended nine pieces of existing Commonwealth legislation, including the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act), to enhance warrant and evidence-gathering powers.

110. While some amendments to the TOLA Bill were made prior to its passage, from a human rights perspective, the Commission considers that significant problems remain with the amendments to federal law implemented by Schedules 2–5 of the TOLA Act.

111. The Commission made 20 recommendations relating to Schedules 2–5 of the TOLA Bill (see Recommendations 34–53 of the Commission's October 2018 submission) that aimed to address the substantial human rights concerns that the Commission had identified. The Commission considers that the Government amendments implemented only two of those 20 recommendations.

5.4 Breadth of ASIO's mandatory assistance powers

112. The Commission is concerned that legislative changes made by the TOLA Act may at present allow ASIO to detain people without effective safeguards such as judicial authorisation.

113. The TOLA Act inserted s 34AAA into the ASIO Act, which allows ASIO to apply for 'assistance orders' relating to computer access. Similar assistance order provisions already exist in the *Crimes Act 1914* (Cth) (Crimes Act) and the *Customs Act 1901* (Cth) (Customs Act).

114. The new s 34AAA of the ASIO Act provides that the Director-General of ASIO 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 enables 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 is imprisonment for a maximum of five years or a fine of $63,000, or both.

115. Assistance orders can only be directed at people who have relevant knowledge of a computer or device, or the measures applied to protect the data. However, they can be made in relation to people who are not suspected of committing any offences, such as the owners and lessees of the relevant devices, employees, system administrators or people who have used the relevant devices.

116. Significantly, unlike the assistance orders that may be made under the SD Act, the Crimes Act and the Customs Act (which are issued by eligible Judges or nominated Administrative Appeals Tribunal members), the assistance orders issued under the ASIO Act are issued by the Attorney-General.

117. Under the new s 34ZH(2) of the ASIO Act, the Government amendments introduced an obligation on the Director-General of ASIO to report to the Attorney-General the extent to which compliance with a compulsory assistance order has assisted ASIO in carrying out its function. The new s 94(2BC) also requires ASIO to list the total number of compulsory assistance orders that the Attorney General has made under s 34AAA(2) within a particular period in its annual report to the Minister, which is tabled in Parliament.

118. New s 34AAA(3C) of the ASIO Act now requires that a request for compulsory assistance be accompanied by a statement setting out the particulars and outcomes of all previous requests (if any) for the making of an order relating to the person specified in the current request. Sections 34AAA(3D) and (3E) of the ASIO Act require that, if the grounds on which an order under s 34AAA was made have ceased to exist, the Director-General must inform the Attorney-General and, if the Attorney-General is also satisfied that the grounds have ceased to exist, the Attorney-General must revoke the order.

119. These reporting and revocation provisions discussed above were inserted into the TOLA Bill by amendments made immediately prior to the passage of the Bill.

120. While the Commission supports the additional reporting, record keeping and procedural changes introduced by the Government amendments, those amendments did not address the significant concerns raised by the Commission, the Inspector-General of Intelligence and Security (IGIS) and the Law Council of Australia about the potential for assistance orders under s 34AAA(2) to authorise effective detention by non-judicial officers.

121. Section 34AAA(3) contemplates that a person subject to an assistance order can be required to attend a specified place to provide assistance. In such circumstances, the assistance order must specify the period within which the person must provide the assistance, but no maximum period is set.

122. As discussed in the Commission's October 2018 submission there is a real question whether a person subject to an assistance order is effectively being detained during the period in which they are required to provide the assistance. While they may not be physically restrained, they are effectively prevented from leaving a specified place prior to the completion of the designated assistance task, under pain of criminal penalties. This might engage the prohibition on arbitrary detention in article 9 of the ICCPR.

123. The assistance order provisions introduced by the TOLA Act 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 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.

Recommendation H

Section 34AAA of the *Australian Security Intelligence Organisation Act 1979* (Cth) should be amended to include protections for persons compelled to

attend or remain in a specified place under an assistance order, in line with Recommendation 48 of the Commission's October 2018 submission.

5.5 Breadth of the concealment of access powers

124. The Commission is concerned that the new 'concealment of access' powers introduced by the TOLA Act remain overly broad.

125. These powers automatically attach to the new computer access warrants issued under the SD Act, as well as warrants issued under the ASIO Act, and permit relevant agencies and ASIO to do 'anything reasonably necessary to conceal the fact that any thing has been done under the warrant'.

126. 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'. This has the potential to apply very broadly.

127. The Government amendments imposed additional obligations on ASIO and relevant agencies to report activities undertaken under the concealment of access provisions relating to expired warrants to the Attorney-General and the Commonwealth Ombudsman respectively.

128. The Commission welcomes these additional reporting obligations from the perspective of transparency, accountability and oversight. However, these amendments are insufficient and do not address the Commission's underlying concern that the new powers allow for highly privacy-intrusive activities to occur long after a warrant has expired.

129. By way of example, it is not difficult to imagine 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 Administrative Appeals Tribunal (AAT) member or, in the case of ASIO warrants, the Attorney-General.

130. In most cases, computer access warrants under the SD Act can only be made after an eligible Judge or nominated AAT member is satisfied that there are reasonable grounds for issuing the warrant. In deciding this, the issuing authority must have regard to certain factors such as the nature and gravity of the alleged offence, the extent to which the privacy of any person is likely to be affected and the existence of any alternative means of obtaining the evidence or information.

131. In the case of computer access warrants issued under the ASIO Act, the Attorney-General can only issue a warrant if he or she is satisfied that there are reasonable grounds for believing that access by ASIO to data held in a computer will substantially assist the collection of intelligence in respect of a matter that is important to security.

132. These thresholds recognise that activities authorised by computer access warrants, and now the ancillary concealment of access powers, are highly privacy-intrusive and should only be permitted when it has been established that there are reasonable grounds for allowing such interference by the state.

133. Given this, the Commission considers that 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. The facts and circumstances of an investigation may have changed considerably in the intervening period.

134. In these circumstances, the Commission recommends that relevant authorities be required to return to an issuing authority to show that privacy intrusive activities are still justifiable with reference to contemporary facts.

Recommendation I

The *Australian Security Intelligence Organisation Act 1979* (Cth) and the *Surveillance Devices Act 2004* (Cth) should be amended so that, if it is not reasonably practicable for 'concealment of access' to occur while a warrant is in effect, or within 28 days of its expiry, law enforcement authorities are required to return to an eligible Judge or nominated Administrative Appeals Tribunal member or, in the case of Australian Security Intelligence Organisation warrants, the Attorney-General for further authorisation

before any of the concealment of access powers introduced by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) can be exercised.

---

1 Revised Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 2.

2 Revised Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 9 [31].

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

4 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].

5 *International Covenant on Civil and Political Rights*, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

6 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].

7 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].

8 For example, the *International Covenant on Economic, Social and Cultural Rights*, opened for signature 16 December 1966, 993 UNTS 3 (entered into force 3 January 1976); *Convention on the Rights of the Child*, opened for signature 20 November 1989, [1991] ATS 4 (entered into force 2 September 1990).

9 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].

10 *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.

11 *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.

12 *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.

13 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].

14 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].

15 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].

[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) 7 [21].

[17] 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].

[18] 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].

[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) 3 [11].

[20] 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].

[21] 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].

[22] United Nations Human Rights Committee, *General Comment No 34: Article 19, Freedoms of opinion and expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) 7 [28].

[23] 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.

[24] 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].

[25] 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).

[26] 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].

[27] 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].

[28] 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].

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

[30] 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].

[31] 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].

[32] 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].

[33] 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].

[34] 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].

[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) [10].

[36] 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].

[37] 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].

[38] This limitation is discussed in detail in the Commission's October 2018 submission at Part 5.2.

[39] The need for a binding independent assessment was also recognised by the Committee in Recommendation 11 of its report on the TOLA Bill.

[40] Under the TOLA Bill, this prohibition applied only to TANs and TCNs, while under the TOLA Act it has been expanded to also include TARs. Pursuant to s 317ZG(2)–(3), building or implementing a relevant weakness includes building a decryption capability, or taking action that would render systemic methods of authentication or encryption less effective.