



22 February 2019

Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

By electronic submission

Dear Committee,

Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

The Australian Human Rights Commission (the Commission) welcomes the opportunity to comment on the Parliamentary Joint Committee on Intelligence and Security (the Committee) inquiry into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (the TOLA Act).

The Commission considers that the effect of the TOLA Act is to permit inappropriately intrusive, covert and coercive powers, without effective safeguards to adequately protect the human rights of law enforcement targets and innocent third parties.

The Commission has made two comprehensive submissions about previous iterations of the TOLA Act. On 12 October 2018, the Commission made a submission to the Committee on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the TOLA Bill), and set out 54 recommendations to improve the Bill's human rights impacts. Earlier, on 10 September 2018, the Commission made a submission to the Department of Home Affairs on an exposure draft of the TOLA Bill (the draft TOLA Bill).

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 Government amendments introduced and passed on 6 December 2018 (the Government amendments). Some of the amendments implemented some of the Commission's previous recommendations, but they did not adequately address the Commission's previously articulated human rights concerns.

The Commission urges the Committee to consider its previous submission on the TOLA Bill dated 12 October 2018 in the course of the present inquiry. It does not repeat the substance of that submission here.

The TOLA Act—or more accurately, the changes to other statutes effected by the TOLA Act—permits significant interferences with the rights to privacy, freedom of expression, due process and freedom from arbitrary detention. At no stage, have the limitations on human rights been demonstrated by the Government to be reasonable, necessary and proportionate to the stated aim of ‘better deal[ing] with the challenges posed by ubiquitous encryption’.

The Commission also notes the very short timeframe in which the Government amendments were introduced and passed—over the course of one day. This did not allow for meaningful parliamentary or public scrutiny of the proposed amendments.

The TOLA Act was also passed one day after the Committee released its report on the TOLA Bill, effectively preventing proper public consideration of the Committee report, and full public scrutiny of the Government amendments, prior to the passage of the Act. Such scrutiny is vital in the case of legislation that seriously 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.

The Commission’s primary recommendation is that the 54 recommendations made in its submission on the TOLA Bill be implemented in full.

In the event that this primary recommendation is not accepted, the attachment to this letter sets out a mitigation strategy in respect of five particularly significant ongoing concerns about the operation of the TOLA Act. This strategy would not fully address the human rights concerns identified by the Commission, but would reduce the negative impact. In summary, the five key concerns highlighted in the attachment to this letter are:

1. the lack of a requirement for judicial authorisation for the giving of Technical Assistance Notices and Technical Capability Notices
2. 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
3. the breadth of ‘relevant objectives’ for which the assistance scheme may be used

4. the breadth of the Australian Security Intelligence Organisation's mandatory assistance powers introduced by Schedule 5 of the TOLA Act
5. the breadth of the 'concealment of access' powers introduced by Schedules 2 and 5 of the TOLA Act.

The attachment does not exhaustively address all of the remaining human rights issues presented by the TOLA Act. Nor does it address the human rights compatibility of all the Government amendments.

Implementing Recommendations B–J contained in this letter would enhance the human rights compatibility of some of the more serious rights interferences permitted by the TOLA Act.

The Commission makes the following recommendations:

Recommendation A

The 54 Recommendations made in the Commission's previous submission to the Parliamentary Joint Committee on Intelligence and Security dated 12 October 2018 should be implemented in full.

In the event that Recommendation A is not adopted, the Commission makes the following recommendations for the reasons in the attachment to this letter:

Recommendation B

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

Recommendation C

In the event that Recommendation B 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 D

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 E

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 F

If Recommendation E 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 G

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 H

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 I

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

Recommendation J

The *Australian Security Intelligence Organisation Act 1979* (Cth) and the *Surveillance Devices Act 2004* (Cth) be amended so that, if it is not

Australian Human Rights Commission

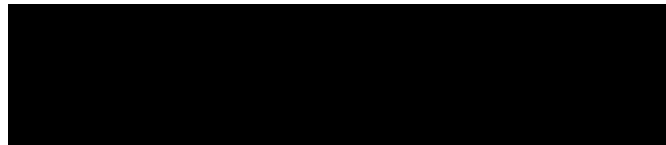
reasonably practicable for 'concealment of access' to occur while a warrant is in effect, or within 28 days of its expiry, law enforcement authorities are required to return to an eligible Judge or nominated Administrative Appeals Tribunal member or, in the case of Australian Security Intelligence Organisation 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.

The Commission would be happy to answer any queries.

Yours faithfully

A solid black rectangular redaction box covering the signature of Edward Santow.

Edward Santow
Human Rights Commissioner

A solid black rectangular redaction box covering the contact information of the Human Rights Commissioner.

Attachment—mitigating five significant human rights concerns about the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)*

Schedule 1 of the TOLA Act

i) Lack of a requirement for judicial authorisation for assistance notices

1. The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)* (the TOLA Act) introduced new powers under which designated communications providers (providers) can be compelled to provide certain government agencies with various forms of technical assistance.
2. As explained in the Commission’s submission on the TOLA Bill dated 12 October 2018 (the previous submission), the Commission considers that:
 - a) agencies should not be able to compel technical assistance without first obtaining independent judicial authorisation (see Recommendation 28 in the previous 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 previous Recommendations 14 and 31)
 - c) providers should have access to judicial review under the *Administrative Decisions (Judicial Review) Act 1977 (Cth)* (see previous Recommendation 30).

The Government amendments do not give effect to these recommendations.

3. The Commission welcomes the amendment to the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the TOLA Bill), introducing the assessment process set out in what is now s 317WA of the Telecommunications Act. This process allows affected providers to request an assessment of whether a proposed Technical Capability Notice (TCN) should be given.
4. 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

Australian Human Rights Commission

making in relation to the giving of notices. The Commission repeats its previous recommendations 14, 28, 30 and 31, for the reasons given in its previous submission.

5. If, contrary to its previous recommendation, 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 TARs, as well as TCNs.
6. 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).¹
7. 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.
8. 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.²
9. Further, the assessment process currently only applies to TCNs and not to other forms of technical assistance. TANs and Technical Assistance Requests (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.
10. 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.
 11. The Commission notes a further change made to the TOLA Bill that altered the oversight of the TCN regime. Section 317TAAA(1) of the Telecommunications Act now 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.
 12. 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 B

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

Recommendation C

In the event that Recommendation B 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 D

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.

ii) 'Systemic weakness' limitation remains ambiguous

13. 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 previous Recommendation 15).

14. 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.

15. 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.

16. Section 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.³ A request or notice will have no effect to the extent that it contravenes s 317ZG(1).

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

Australian Human Rights Commission

- (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.
18. 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.
19. 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.
20. 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.

21. 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.
22. 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.
23. 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.
24. 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.
25. 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'.

26. 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.
27. The Commission considers that s 317G should be amended to prevent assistance measures that negatively 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.
28. 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.
29. 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.
30. However, a possible alternative reading of ss 317ZG(4A)–(4C) would give those provisions no effect, as explained below.
31. 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'.
32. Subsection 317ZG(4A) then seeks to reintroduce such 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).

33. 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.
34. 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 ss 317ZG(4A)–(4C) having no effect.
35. 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.
36. 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 Senate has agreed to this amendment. This amendment would remove the ambiguity about the interaction between ss 317B and 317ZG(4A)–(4C), and appears to address several of the Commission's concerns. However, this amendment is not currently before the Committee, and, in the absence of further information, the Commission is not in a position to say whether it would address all of its concerns about the operation of the 'systemic weakness' limitation.

Recommendation E

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 F

If Recommendation E 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.

iii) 'Relevant objectives' too broad

37. 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.
38. 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.
39. 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.
40. 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 previous Recommendation 6 made by the Commission 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.

41. '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.
42. 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 previous Recommendation 6). That provision includes offences punishable by imprisonment for life, or a period of at least seven years.
43. 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.
44. 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 G

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 H

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

45. In its submission to this Committee dated 12 October 2018, the Commission raised serious concerns about the human rights implications of Schedules 2–5 of the TOLA Bill. Schedules 2–5 proposed to 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 sought to amend nine pieces of existing Commonwealth legislation, including the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act), to enhance warrant and evidence-gathering powers.
46. 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. These issues have received comparatively less public attention than those arising from Schedule 1 of that Act, but are of comparable importance.
47. The Commission made 20 recommendations relating to Schedules 2–5 of the TOLA Bill (see previous Recommendations 34–53) that aimed to address the substantial human rights concerns that the Commission had identified. The Government amendments that form the subject of this inquiry can be said to implement only two of those 20 recommendations.

iv) Breadth of ASIO’s mandatory assistance powers

48. The Commission is concerned that legislative changes made by the TOLA Act may presently allow ASIO to detain people without effective safeguards such as judicial authorisation.
49. 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).
50. 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

Australian Human Rights Commission

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.

51. 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.
52. 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.
53. 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.
54. 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.
55. These reporting and revocation provisions discussed above were inserted into the TOLA Bill by amendments made immediately prior to the passage of the Bill.
56. 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

Australian Human Rights Commission

Law Council of Australia about the potential for assistance orders under s 34AAA(2) to authorise detention by non-judicial officers.

57. 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.
58. As discussed in the Commission's submission dated 12 October 2018, 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 *International Covenant on Civil and Political Rights*.
59. 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 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.

Recommendation I

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

v) Breadth of the concealment of access powers

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

Australian Human Rights Commission

61. 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'.
62. 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.
63. 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.
64. 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.
65. 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 Administrative Appeals Tribunal (AAT) member or, in the case of ASIO warrants, the Attorney-General.
66. 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.

67. 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.
68. 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.
69. 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.
70. 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 J

The *Australian Security Intelligence Organisation Act 1979* (Cth) and the *Surveillance Devices Act 2004* (Cth) 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.

Improvements to the Bill

71. The Commission welcomes the following changes made by the Government amendments, which go some way to enhancing the human rights safeguards in the TOLA Act:

- a) the requirement for statutory review by the Independent National Security Legislation Monitor—this implements previous Recommendation 54
- b) the narrowed definitions of ‘acts or things’ and ‘listed help’, so that they are exhaustive with respect to TANs and TCNs—this partially implements previous Recommendation 3, noting that the ‘listed acts or things’ that a provider may be asked to do under a TAR still do not appear to be exhaustively defined given the operation of s 317G(6) of the Telecommunications Act
- c) the revised decision-making criteria for giving TARs, TANs and TCNs, including making it mandatory for the decision maker to consider whether a request or notice is necessary as well as whether it is the least intrusive form of industry assistance as far as any impacts on third parties are concerned—this implements previous Recommendation 8 and partially implements previous Recommendation 10, though it does not address all of the Commission’s concerns, because:
 - these changes do not go so far as to *require* that the decision maker be satisfied on reasonable grounds that the human rights impacts including interferences with privacy are reasonable, necessary and proportionate
 - a decision maker is required to consider only whether a particular request or notice is the ‘least intrusive’ form of industry assistance, rather than the least intrusive measure available having regard to other law enforcement capabilities as a whole
- d) the additional safeguards relating to TARs as follows, which implement the Commission’s previous Recommendations 11, 16 and 18:
 - the application of the ‘systemic weakness’ limitation in s 317ZG of the Telecommunications Act to TARs, which previously applied only to TANs and TCNs
 - the introduction of the decision-making criteria in ss 317JAA and 317JC, which prevent a TAR being issued unless the decision maker is satisfied that the request is reasonable and

- proportionate, and that compliance is practicable and technically feasible
- the application of the general limits in s 317ZH to TARs, which previously applied only to TANs and TCNs
 - e) minor revised public reporting requirements, including the introduction of a requirement for annual reports under s 317ZS of the Telecommunications Act to state the kinds of serious Australian offences for which assistance powers have been used—this is a small improvement, but does not implement previous Recommendation 32 which recommended detailed public reporting of statistical and other information about the use of TARs, TANs and TCNs
 - f) improved oversight powers for the Commonwealth Ombudsman and IGIS, including through additional notification obligations placed on agencies when they utilise certain powers—this partially implements previous Recommendation 27
 - g) the introduction of the requirement in s 317MAA of the Telecommunications Act to advise a provider of their right to make a complaint with respect to a TAN—this partially implements previous Recommendation 19 but does not go so far as to require detailed written notification to providers of relevant information; the requirement also does not apply to TARs or TCNs
 - h) the introduction of a 12 month maximum time limit for the duration of TANs and TCNs—this partially implements previous Recommendations 12 and 13, noting that there is no time limit applicable to TARs and no limit on the number of notices that can be issued as a whole
 - i) increased reporting and record-keeping obligations by ASIO and law enforcement agencies regarding the exercise of powers introduced by Schedules 2–5 of the TOLA Act
 - j) the extension of limitation provisions relating to material loss and material interference with the lawful use of a computer in ASIO and SD warrants to concealment activities—this implements previous Recommendations 40 and 41.
72. Notably, there have been no amendments to address the Commission’s concerns regarding the provision of broad civil and criminal immunities to providers who comply or purportedly comply with TARs, TANs and TCNs (see previous Recommendations 21–24.) The Commission’s previous recommendation that the TOLA Bill adopt a harms-based approach to secrecy, and to expressly permit disclosure for certain public interest or

integrity purposes, has also not been addressed (see previous Recommendations 25–27).

73. Despite the above improvements, the Commission continues to hold serious concerns that the legislative changes enacted by the TOLA Act are not sufficiently targeted and delimited to be compatible with international human rights law.
74. The Commission supports further review and reform of the TOLA Act, consistent with its previous submission on the TOLA Bill and all 54 of its previous recommendations.

¹ This limitation is discussed in detail in the Commission’s previous submission at Part 5.2.

² The need for a binding independent assessment was also recognised by the Committee in Recommendation 11 of its report on the TOLA Bill.

³ 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.