Australian Government
Department of Home Affairs

Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Parliamentary Joint Committee on Intelligence and Security

Supplementary submission

Table of Contents

Introduction

1. This supplementary submission, provided to the Parliamentary Joint Committee on Intelligence and Security (the Committee) inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, considers in detail the issues raised by public submissions concerning Schedules 2 – 5.

Schedule 2 – Computer access warrants

2. Traditionally, the *Surveillance Devices Act 2004* (Cth) (SD Act) has permitted devices such as mobile phones to be accessed via warrant. However, this warranted access has only enabled '*view only*' access. Essentially, once the surveillance device is installed on the mobile phone, law enforcement cannot access files or file structure, only view what the person of interest is *currently* doing. With the incredible uptake of technology, this is becoming increasingly restrictive to law enforcement efforts. For example, a person who accesses child sexual abuse material may have large collections on their device and be sharing this material with individuals overseas. This information may not be easily detected purely through the viewing of the device. The added complexity of encryption means that accessing data on the phone both within the file structure of the device and before encryption takes place can be key to obtaining vital evidence to investigate and prosecute serious crime.
3. The Bill permits law enforcement, security and intelligence agencies to seek Computer Access Warrants (CAWs) under a range of circumstances, such as the investigation of serious crimes (defined as offences with a minimum penalty of 3 years' imprisonment or above), monitoring compliance with control orders, integrity operations and recovery orders to assist in the location and safe recovery of children. The execution of a CAW is done covertly and remotely, limiting the interference with property and risk of harm to law enforcement officers. These changes modernise the evidence and intelligence collection capabilities of Australia's key agencies and will facilitate the lawful collection of data in a more accessible state.
4. Questions or issues raised by submissions to the Committee are responded to below.

Permitting telecommunications interception for the purposes of a computer access warrant

5. Access to mobile devices is increasing, as is their use in facilitating crimes or acts of terrorism. As a consequence, accessing such devices is incredibly important to ensuring our law enforcement and national security agencies have effective powers to combat those threats. However, new mobile devices are constantly being created, and respective software subject to near daily updates. Computer access capabilities do not work in a vacuum and require some degree of knowledge and interaction with the telecommunications system before execution. As a consequence, it may be necessary to use interception capabilities in order to technically enable computer access. The *Telecommunications (Interception and Access) Act 1979* (TIA Act) has been amended in order to provide for this incidental interception.
6. The stated objective of this measure is two-fold: to enhance the operational effectiveness of the use of CAWs, and to ensure that multiple warrants are not required to achieve a single purpose – that being the execution of a CAW. If law enforcement agencies and ASIO need to meet thresholds for the existing interception regime this may mean that a valid CAW cannot be executed, or significant delays may be imported into the process, despite the fact that the interception is purely incidental and not for independent evidence or intelligence collection. We note that the threshold to obtain a CAW will be offences with a maximum of 3 years' imprisonment or more in most instances. The existing

threshold for interception warrants is generally offences with a maximum 7 years' imprisonment or more. Delay, or inability, associated with an inability to undertake incidental interception may result in either significant loss of evidence or the continuation of serious crime.

7. In effect the amendments do not lower the threshold for primary interception as the amendments do not permit interception independently. This is consistent with the general exceptions to the prohibition against interception in section 7 of the TIA Act. Subsection 7(2) exempts a number of legitimate activities that require the incidental interception of communications, including 'the interception of a communication where the interception results from, or is incidental to, action taken by an ASIO employee, in the lawful performance of his or her duties' for the purposes of detecting whether a listening device is being used.
8. Strict prohibitions apply to the use of any information obtained through this incidental interception and use and disclosure in the TIA Act is tied to the primary purpose of the CAW. Should an agency wish to pursue interception to collect evidence or intelligence in its own right they must seek an interception warrant.
9. Incidental interception is rationally connected to computer access and is a necessary, proportionate and reasonable measure to ensure available judicially approved powers can actually be executed.

Emergency authorisations and computer access warrants

10. The use of emergency authorisations for surveillance devices is not new. Since 2004, emergency authorisations have been available for the broader set of surveillance device powers under the SD Act.
11. Emergency authorisations are available only in special circumstances, namely where there is imminent risk of serious violence or substantial property damage, where it will assist relating to a recovery order, and where there is a risk of loss of evidence. In each of these special circumstances, the use of an emergency authorisation must be immediately necessary to achieve the stated purpose and it must be demonstrated that it is not practical to apply for a CAW.
12. Safeguards exist to ensure that emergency authorisations are necessary and proportionate. Within 48 hours after an emergency authorisation is given by an authorising officer, there must be an application to an eligible Judge or AAT member for approval. In deciding whether to approve this application, an eligible Judge or AAT member must, being mindful of the intrusive nature of the use of a surveillance device, consider various things, such as urgency in relation to the stated purpose (e.g. risk of serious violence to a person), alternative methods, and whether or not it was practicable in the circumstances to apply for a surveillance device warrant. These same protections and processes apply to emergency authorisations for a CAW.
13. Information gathered as part of an emergency authorisation is considered '*protected information'* and is subject to the strict use and disclosure provisions that ordinarily exist for information obtained from powers exercised under the SD Act. Criminal liability is attached to unauthorised disclosure of protected information under the SD Act.
14. The availability of the use of computer access powers under an emergency authorisation is proportionate and is necessary to ensure that, in special circumstances, the computer access powers can be used for the purposes of public safety and national security. The powers strike a reasonable balance between protecting the community and the interests of the public and respect for individual privacy.

Inconsistency between computer access warrant emergency authorisations and existing attributes of emergency authorisations under section 32

15. Submissions have raised that there is an apparent inconsistency between current surveillance device powers and the proposed CAWs under section 32. Under proposed paragraph 27E(2)(h) of the SD Act, a CAW will permit agencies to intercept communications (as explained above). However, submissions have indicated that this is inconsistent with the existing subsection 32(4) of the SD Act which states that '*nothing in this Part authorises the doing of anything for which a warrant would be required under the TIA Act*'.

16. The Department views that this is not inconsistent with the existing subsection 32(4) of the SD Act as the act of interception is permitted by a warrant under the SD Act, not the TIA Act. The justification for doing so is explained above. Proposed subsection 32(2A) of the SD Act provides that an emergency authorisation may authorise anything that a computer access warrant may authorise. A computer access warrant may authorise intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing anything specified in the warrant in accordance with proposed subsection 27E(2) of the SD Act.

    The Department does not think that there is any inconsistency between existing subsection 32(4) and proposed subsection 27E(2)(h) because a warrant would not be required under the TIA Act to authorise the type of activity described in paragraph 27E(2)(h). That is, a warrant would not be required under the TIA Act in order to intercept communications passing over a telecommunications system if the interception is for the purposes of doing something specified in CAW.

Use of force and computer access warrants

17. The proposed amendments enabling the necessary and reasonable use of force are required due to likely eventualities that officers may face while executing a warrant. For example, it may be necessary to use force against a door or a cabinet lock to access a thing on the premises or to use force to install or remove a computer. In the case of force against a person, its use is constrained on the face of the legislation to circumstances where force is required to execute the CAW. For instance, it may be necessary to use reasonable force if a person is obstructing a doorway into the warrant premises and an officer needs to move past them.

18. The absence of a power to use reasonable and necessary force could potentially lead to civil action or criminal charges should a law enforcement officer do acts or things against a person proportionate to what is contemplated by warrant. Reasonableness and necessity cause its use to be conditional in all circumstance.

19. Submissions highlight that the use of force should be specifically excluded in relation to telephone interception. However, it is long standing practice that entry onto premises may be necessary where it would be impractical or inappropriate to intercept communications in respect of a device otherwise than by using equipment installed on specified premises. This may be due to technical reasons connected with the operation of the service or the telecommunications system of which the service is part, or because the execution of the computer access warrant as a result of action taken by an officer of a carrier might jeopardise the security of the investigation. Accordingly, it is reasonable and necessary to ensure that law enforcement officers undertaking these activities can do so with appropriate authorisations around the use of force.

Availability of provisions which permit law enforcement and intelligence agencies to conceal their activities to execute a computer access warrant.

20. Undertaking surveillance activities on an electronic device may alter data, or leave traces of activity, on that device. This may allow for alleged terrorists and criminals to recognise the lawful intrusion and effectively change the way they communicate for the purposes of avoiding law enforcement (e.g. recognition may lead to reverse engineering the police capabilities and methodology leading to individuals avoiding certain technologies or undertaking counter-surveillance activities). Accordingly, the concealment of the execution of a CAW is vital to the exercise of the powers under Schedule 2, and indeed, the existing powers under the *Australian Security Intelligence Organisation Act 1979* (ASIO Act).
21. In the event that law enforcement agencies and ASIO are not able to conceal, there is significant risk to the exposure of police technologies and methodologies. This could reduce opportunities for agencies to prevent serious crime and acts of terrorism.
22. There is a clear rational connection between the availability of concealment provisions both under this Bill and within the ASIO Act and the necessary pursuit of the legitimate objectives of public safety, public order and national security.
23. The measures are subject to limitations, safeguards and oversight mechanisms designed to ensure that the proposed and existing measures are used proportionately, reasonably and only as necessary. For example, the proposed CAWs under the Bill are subject to the requirement for judicial authority and oversight by the Commonwealth Ombudsman, and the existing ASIO CAWs are subject to ministerial oversight (approval required by the Attorney-General) and oversight by the Inspector-General of Security and Intelligence (IGIS).

Compulsory assistance to law enforcement relating to data

24. Proposed section 64A is similar to section 3LA of the *Crimes Act 1914* (Crimes Act) and ensures that law enforcement agencies that have a warrant for computer access will be able to compel assistance in accessing devices.
25. Although the SD Act provides for the issuing of warrants permitting covert activity, there may be circumstances in the course of an investigation where a person who is not the suspect or target will have knowledge of a computer system and be able to provide access to relevant data, without compromising the covert nature of the investigation. Alternatively, there may be a point in the investigation where the benefits of compelling information from a person in order to enable access to data outweigh the disadvantages of maintaining the secrecy of the investigation.
26. The different purpose and functions of ASIO and law enforcement agencies is the key reason for the contrasting limitations between the compulsory assistance regimes under section 34AAA and 64A of the Bill. The assistance order under section 64A is intended to support the proposed computer access warrants in Schedule 2. The limitations in 64A reflect the fact that this power is available to Commonwealth, state and territory law enforcement agencies. The compulsory assistance orders under section 34AAA are intended to support ASIO's broader functions and operations. Police already have assistance orders under 3LA which support access to more generalised search warrants. Allowing compulsory assistance orders to be issued to those persons that are unknowingly or unintentionally involved in activities that are contrary to ASIO's functions is necessary and proportionate considering the seriousness of those matters before ASIO. Compulsory assistance provided by these persons may be crucial to enable ASIO investigations into threats against Australia.

Restrictions on compensation to actions resulting from the execution of a computer access warrant

27. The Government is considering whether amendments are necessary to bring computer access warrants in line with the other surveillance device compensation under section 64 of the SD Act.

Assistance to foreign countries and tribunals in relation to data held in computers

28. The reforms in the Bill will strengthen the available tools for the purposes of mutual assistance assisting in the enforcement of foreign serious crime and terrorism. These crimes frequently transcend traditional borders, involving large criminal networks across the globe. International crime cooperation must evolve to ensure that tools that would otherwise be available to domestic law enforcement can be used to assist foreign countries and international bodies where it is appropriate and reasonable to do so.
29. The stated objective of these amendments is to ensure that no matter the origin of serious crime and terrorism, Australian law enforcement can assist foreign law enforcement agencies and international bodies through mutual assistance processes to undertake investigatory powers within Australia.

Part 1, Schedule 2: Mutual Assistance in Criminal Matters

30. Schedule 2 amendments to *Mutual Assistance in Criminal Matters Act 1987* (MACMA) pursue the objective of enhancing public safety, public order and national security by assisting foreign countries where appropriate to do so. What assistance is appropriate is shaped by the current mandatory and discretionary grounds of refusal within MACMA. Australia's mutual assistance domestic framework ensures that there are human rights protections in place for the purposes of any incoming request from a foreign country and stand as an appropriate yardstick in determining whether undertaking powers, such as that under Part IIIBB would meet reasonable community expectations as to balancing human rights and law enforcement/national security interests.
31. For example, section 8 of MACMA provides that where a person has been charged, arrested, detained or convicted of an offence that could result in the death penalty, mutual assistance must be refused unless there are '*special circumstances'*. The term 'special circumstances' is not defined in the MACMA but its Explanatory Memorandum envisages that it may include where a requesting country has provided an undertaking that the death penalty will not be imposed, or if it is imposed, will not be carried out. Where a person has not yet been charged, arrested, detained or convicted, there is a general discretion to refuse assistance.
32. Section 8 of MACMA provides for various other protections including the ability to refuse requests:
    a. which would involve investigating, prosecuting, punishing or otherwise causing prejudice to a person on account of the person's race, sex, sexual orientation, religion, nationality or political opinions.
    b. where there are substantial grounds for believing that if the request was granted the person would be in danger of being subject to torture. The discretion in paragraph 8(2)(g) of MACMA can cover any concerns about cruel, inhuman or degrading treatment of punishment.
    c. where the person has already been acquitted, pardoned or undergone punishment for the offence.
33. The Bill also provides appropriate safeguards for the use of personal information collected and disclosed. Use of the new power requires both the Attorney-General's approval and the approval of a

judicial officer or AAT member. For example, if a foreign country requests access to data held on a computer, the Attorney-General must be satisfied of certain things before authorising an eligible law enforcement officer to apply for a computer access warrant. Part IIIB includes specific safeguards such as ensuring a minimum threshold (3 or more years' imprisonment) and a tangible link between the request and a device in Australia. Further, in addition to the general power to impose conditions on the provision of assistance in s9 of MACMA, the proposed amendments enable the Attorney-General to request appropriate undertakings in relation to:

a. the information is used only for the purposes in which it was sought;

b. destruction requirements subsequent to its use; and

c. any other matter the Attorney-General may consider appropriate.

34. These amendments are made for the purpose of international law enforcement in relation to serious crimes and are limited to interferences that are necessary to achieve this. Computer access powers are a vital tool not only domestically but also where those powers may be exercised by a foreign jurisdictions law enforcement to assist Australian investigations into serious crime and terrorism.

Including information obtained from a domestic investigation as part of the definition of 'Protected information'

35. The specific inclusion of computer access information as part of the definition of '*Protected information'* under 13A of MACMA accords with the existing practice of lawfully obtained surveillance device information and intercepted information. Notably the Attorney-General can only provide such an authorisation in relation to an offence which is a serious offence punishable by a maximum penalty of imprisonment for 3 years or more. In giving such an authorisation the Attorney-General may specify the uses to which the material may be put.

36. The provision of that information for the purposes of mutual assistance will continue to be governed by the existing safeguards under sections 8 and 9 of MACMA described above.

Calls for an independent review of MACMA

37. The Department and Australia's Central Authority within AGD are satisfied with the current operation of MACMA. Australia's mutual assistance regime and procedures are frequently considered and assessed. The operation of Australia's mutual assistance laws are subject to Parliamentary scrutiny through the Joint Standing Committee on Treaties hearings for new treaties and reports by the Parliamentary Joint Committee on Human Rights. Australia conducted a comprehensive review of its mutual assistance arrangements which resulted in amendments that were passed in 2012.

38. As noted above, there is also a comprehensive array of safeguards and oversight mechanisms which ensure any assistance in criminal matters which relate to requests from foreign countries accord with the fundamental rule of law principles and international obligations.

What constitutes 'special circumstances'

39. Submissions have highlighted the uncertainty around the meaning of 'special circumstances' within MACMA in relation to the death penalty. MACMA provides that where a person has been charged, arrested, detained or convicted of an offence that could result in the death penalty, mutual assistance must be refused unless there are 'special circumstances'. The term 'special circumstances' is not defined in the MACMA but its Explanatory Memorandum envisages that it may include where a requesting country has provided an undertaking that the death penalty will not be imposed, or if it is imposed, will not be carried out. Where a person has not yet been charged, arrested, detained or convicted, there is a general discretion to refuse assistance.

40. The Department understands from Australia's Central Authority that the scope of 'special circumstances' is required to be sufficiently broad enough to ensure that a range of circumstances can be taken into consideration when the Attorney-General, or his/her delegate, decides whether to refuse a request from a foreign country. For example, the Explanatory Memorandum also envisages special circumstances including where the assistance provided is exculpatory.

Part 3, Schedule 2: International Criminal Court and International War Crimes Tribunals

41. The amendments in Part 3 of Schedule 2 will align the *International War Crimes Tribunals Act 1995* (IWCTA) and the *International Criminal Court Act 2002* (ICC Act) with MACMA with respect to computer access warrants on behalf of the International Criminal Court or an International War Crimes Tribunal. This will allow assistance to be provided to those bodies, who investigate serious crimes such as genocide and crimes against humanity. These bodies are not empowered to impose the death penalty.
42. In addition to the safeguards contained in the SD Act, the provision of such assistance will be subject to the safeguards contained in the ICC Act and IWCTA, for example:
    a. as with the MACMA, both Acts will require the Attorney-General's authorisation and judicial (or AAT) involvement in order for a computer access warrant to be issued
    b. a request under the IWCTA cannot be granted if it would prejudice Australia's sovereignty, security or national interest or there are special circumstances justifying non-compliance; and
    c. a request under the ICC Act may be refused where the request involves national security.

Concealment and computer access warrants

43. Undertaking surveillance activities on an electronic device may alter data, or leave traces of activity, on that device. This may allow for alleged terrorists and criminals to recognise the lawful intrusion by law enforcement agencies and effectively change the way they communicate for the purposes of avoiding law enforcement (e.g. recognition may lead to reverse engineering the police capabilities and methodology, leading to individuals avoiding certain technologies or undertaking counter-surveillance activities). Accordingly, the concealment of the execution of a CAW is vital to the exercise of the powers under Schedule 2, and indeed, the existing powers under the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). Concealment activities include:
    - Entry and exit to premises, including third-party premises,
    - Removal and return of computers or other things from premises,
    - The use of other computers or communications in transit, including if necessary adding, copying, deleting or altering data in the computer or the communication in transit,
    - The interception of telecommunications, and
    - Other things reasonably incidental to these activities.
44. In the event that law enforcement agencies and ASIO are not able to conceal their activities, there is significant risk to the exposure of police technologies and methodologies. This could reduce opportunities for agencies to prevent serious crime and acts of terrorism.
45. There is a clear rational connection between the availability of concealment provisions both under this Bill and within the ASIO Act and the necessary pursuit of public safety, public order and national security.

46. The measures are subject to limitations, safeguards and oversight mechanisms designed to ensure that the proposed and existing measures are used proportionately, reasonably and only as necessary. For example, the proposed CAWs under the Bill are subject to the requirement for judicial authority and oversight by the Commonwealth Ombudsman, and the existing ASIO CAWs are subject to ministerial oversight (approval required by the Attorney-General) and oversight by the IGIS.

Automatic concealment authorisation

47. Concealment activities do not require the approval from the Attorney-General or Director-General, eligible Judge or nominated AAT member for specific concealment activities. Submissions to the Committee have raised that there should be specific approval to avoid unnecessary or disproportionate use of the powers, and that this will ensure that ASIO or law enforcement agencies carefully plan how the powers can be used to meet the relevant intelligence or law enforcement objective.
48. Requiring specific approval for each concealment activity may be impractical or impossible given the changing landscape that may be involved in concealment activities and the use of a CAW. For example, as the entity that installed the original CAW and monitored its use, agencies will have peculiar knowledge about the necessary concealment methods and may need to undertake concealment efforts urgently in response to the risk of discovery. Further, the methods being used to conceal electronic surveillance may not necessarily be known until the law enforcement agency has access to the device, making prior authorisation impracticable.
49. Submissions raise that not requiring approval for specific concealment activities may lead to unnecessary or disproportionate use of the powers. Existing oversight mechanisms such as Commonwealth Ombudsman or the IGIS (in the case of ASIO) provide sufficient oversight to ensure there is accountability for any unnecessary or disproportionate use of the proposed concealment powers.

Certain acts not authorised

50. Submissions to the Committee further raised that the safeguards under the proposed concealment provisions for both the ASIO Act and the SD Act are not safeguards in reference to the concealment powers. The '*certain acts not authorised'* safeguards under subsection 27E(5) will apply to the execution of a CAW. The acts not authorised relate to the addition, deletion or alteration of data, or the doing of anything, that is likely to interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. The concealment provisions specifically allow for these acts as part of the concealment where reasonably necessary to conceal the execution of a CAW. To maintain operational integrity it may be necessary to conceal activities through manipulation of data and while the safeguards don't apply here, the purposes for which they are abrogated are very limited.

Duration of the concealment provisions after the expiry of the computer access warrant

51. Subsection 27E(7) details activities which law enforcement agencies can undertake to conceal the execution of a CAW. Specifically 27E(7)(j) sets out that these activities can be done at any time while the warrant is in force or within 28 days after it ceases to be in force or at the most reasonably practicable time post the 28 day period. The extended duration in which law enforcement agencies can undertake concealment activities recognises that during the period of the warrant and shortly after may not provide sufficient opportunities to conceal execution, including where necessary, the retrieval of capabilities.

Removal of computers or other things from premises

52. Schedule 2 permits the temporary removal of computers or other things from a premises subject to a CAW granted under the ASIO Act or the SD Act.

Temporary removal in ASIO warrants

53. Subsection 25A(4)(ac) of the ASIO Act will allow ASIO to remove a computer or other thing from the premises where a CAW has been executed for the purpose of doing what is specified in the warrant. This is necessary where ASIO may require the use of specialised equipment located off-site in order to access or analyse data, for instance. Given the purposive language of the section, the category of other things which may be removed is limited to things that are, in some way, needed to execute the CAW. The ability to retain the removed items is limited to the duration of the warrant and the Attorney-General is empowered to specify conditions relating to the return of the computers and other things.

Temporary removal in SD warrants

54. The ability to temporarily remove a computer or other thing from a premises under a CAW operates similarly under the SD Act as under the ASIO Act. One key difference is that CAWs issued under the SD Act must be authorised by an eligible Judge or nominated AAT member rather than the Attorney-General. As with ASIO CAWs, the rationale for allowing computers or other things to be temporarily removed from a premises is to allow law enforcement to use specialised equipment or tools located off-site to execute the warrant.

Oversight mechanisms and reporting requirements

55. The ASIO Act and SD Act both contain substantial oversight and reporting requirements which will apply to the new powers granted by this Bill.

Oversight in the ASIO Act

56. The existing CAWs available in section 25A of the ASIO Act are limited to circumstances where there are reasonable grounds to believe that the data sought by the warrant will substantially assist the collection of intelligence in respect of a matter that is important in relation to security. This limits ASIO's access to CAWs to circumstances where they can be reasonably expected to contribute to an ASIO investigation. The requirement that the Attorney-General be satisfied that there are reasonable grounds to believe the issue of this warrant will substantially assist ASIO's collection of intelligence is the appropriate standard of authorisation as it is consistent with the standard throughout the ASIO Act. Given the high national security content of ASIO's activities authorisation through the Attorney-General (first law officer and an executive member intimately familiar with Australia's national security landscape) rather than a judge is a consistent feature of the legislation. The Director-General of ASIO is required to report to the Attorney-General regarding warrants issued under Division 2 of the ASIO Act on the extent that the warrant has assisted ASIO in carrying out its functions. The exercise of ASIO's powers are directly overseen by the IGIS and existing reporting requirements in the ASIO Act attach to the execution of warrants. There is therefore extensive ministerial and independent scrutiny of ASIO activities.

Oversight in the SD Act

57. The CAWs that will be available under section 27A of the SD Act are limited to the investigation of 'relevant offences' defined under the SD Act as offences which attract a maximum penalty of 3 years of imprisonment or more. This will limit the category of offences that may be investigated with new SD Act CAWs to those offences whose investigation is already oversighted by the SD Act. CAWs granted

under the SD Act must be authorised by an eligible Judge or nominated member of the AAT and this provides judicial oversight over the exercise and operation of these warrants. These independent authorities must take into account core considerations like privacy and the availability of alternative methods before issuing the warrant.

58. Additionally, the Commonwealth Ombudsman is empowered to investigate the administration of the SD Act and the law enforcement agencies that exercise powers under it. The SD Act also places reporting requirements on law enforcement agencies when a warrant is issued or an emergency authorisation is given and requires warrant statistics to be reported to the Minister for Home Affairs for the purpose of generating an annual report. Further, to protect the privacy rights of individuals subject to an SD Act warrant, information collected under the SD Act is 'protected information'[1] and its disclosure is an offence.

Section 64A – Compulsory assistance powers

59. Under section 64A of the SD Act, law enforcement will have the ability to apply to an eligible Judge or AAT member for an order to require a person with knowledge of a computer or a computer system to provide information or assistance that is reasonable and necessary to allow access to relevant data. This power is similar to the powers already available under section 3LA of the *Crimes Act 1914* and section 201A of the *Customs Act 1901*.

Self-incrimination

60. The Department does not consider that assistance orders engage the common law right to freedom from self-incrimination on the basis that an assistance order does not compel a person to confess guilt or provide evidence against interest. Assistance orders merely allow law enforcement the ability to search a device. This is not dissimilar from a search warrant executed on a premises where there is no argument that the right is not engaged. Assistance orders do not compel an individual to go into their device and disclose information or documents. It simply provides an avenue for law enforcement and national security agencies to lawfully gain access to that device, so that a lawful search of the device may be conducted as necessary. Further, assistance orders must be independently authorised.

Proportionality of penalties

61. The penalty for non-compliance with an assistance order provided by section 64A is set at a maximum of 10 years imprisonment or 600 penalty units. This penalty is proportionate to many of the serious offences that may be investigated with the help of an assistance order granted under this provision. In order for the compulsory nature of the assistance order to be realised, it is necessary that the penalty for non-compliance be able to be matched with that of the offence being investigated or represent a sufficient deterrent for persons attempt to hide evidence of serious criminality. Importantly, this section does not prescribe a mandatory minimum penalty but a maximum. This ensures that judges, in sentencing, have the discretion to appropriately penalise offenders for non-compliance commensurate to the alleged offence to which the assistance order related.

[1] '*Protected information'* is a class of information protected under the SD Act which relates to information obtained from the use of a surveillance device, or relates to the use of the surveillance device (e.g. warrant information); see, section 44 of the SD Act.

Schedule 3—Search warrants issued under the *Crimes Act 1914* & Schedule 4—Search warrants issued under the *Customs Act 1901*

Search warrant access to third-party computers or communications in transit: consideration of human rights and other methods of access under the *Crimes Act 1914* (Cth), and the *Customs Act 1901* (Cth)

Requirement that law enforcement consider alternative methods of access

62. The Bill enhances the existing search warrant frameworks under the Crimes Act and the *Customs Act 1901* (Cth) (Customs Act). These measures will improve the ability of law enforcement agencies to overtly access data and search electronic devices subject to a search warrant and facilitate forensic best practice when it comes to examining and processing this information.

63. The Bill enables executing officers to obtain access to data or a device remotely, including by using other computers or communications or by adding, deleting and copying data. These measures require that the actions taken under that warrant by the executing officer are subject to the consideration of reasonableness, with specific regard to the use of other methods (if any) of obtaining access to the relevant data under sections 3F(2B)(c) (Crimes Act) and 199B(2)(c) (Customs Act). It is therefore not an arbitrary decision to utilise third-party computers or communications and is grounded by what is reasonably appropriate at the time.

64. Further to the considerations outlined above, the operational reality of agency activities will always carry a degree of the unknown. It would be difficult for an issuing authority to have a sufficient degree of awareness of the investigative reality to properly consider alternative avenues of access when they are authorising the warrant. Therefore, it is more appropriate that the consideration of the degree of reasonableness of access to be undertaken by an *executing officer*, who would be sufficiently aware of other methods of access that may be available to them. Accordingly, the reasonableness requirement only permits access to third-party computers, or communications in transit, where other methods have already been considered is a sufficient safeguard.

Impact on the human rights of third parties

65. The Government undertook extensive consultation, including a two stage consultation process on the text of the Bill. This process was productive and led to significant amendments that addressed key concerns and reinforced the policy intent of the Bill. Importantly, the consultation process allowed government to clarify the strong safeguards and limitations in the Bill that carefully ensure that the privacy of Australians is not compromised, the security of digital systems is maintained and agency powers are utilised appropriately.

66. It is the Department's view that the consideration of human rights has been sufficiently addressed as outlined in the Bill's statement of compatibility, and the detailed Government response provided to the Parliamentary Joint Committee on Human Rights (PJCHR) report. This response is available at **Attachment A**.

The proportionality of increased penalty provisions of assistance orders

67. Law enforcement have noted that the current assistance order regime is insufficient to gain access to devices that may harbour evidence relating to a serious offence. Where offenders are aware that evidence on their device may lead to a sentence greater than the existing penalty, they are more likely to refuse the assistance order in place of the heavier penalty. An example is the 2016 prosecution of an individual who was convicted of 13 charges relating to the control of multiple child sexual abuse websites on the 'dark web' which he used to access a network where he controlled, distributed and facilitated the production of child pornography material. He received total effective sentence of 15 years six months' imprisonment with a non-parole period of 10 years. For the offence under section 3LA, he was sentenced to six months' imprisonment, which must be considered in the context of the overall sentence.
68. The Bill increases the penalty for simple offences of non-compliance with an assistance order from two years imprisonment or 120 penalty units, to five years imprisonment or 300 penalty units, or both (see subsection 3LA(5)). The Bill also introduces a penalty for serious/aggravated offences of 10 years imprisonment or 600 penalty units, or both (see subsection 3LA(5)). This represents a tiered approach to enforcement. It is important to note that the aggravated penalty is only available where the underlying investigation relates to a serious offence (defined as an offence attracting two years or more imprisonment) or serious terrorism offences. The intention is that the revised penalties reflect the gravity of non-compliance.
69. The Department's view is that the new measures are proportionate in that they provide for a maximum penalty, and judicial officers will maintain discretion to decide what penalty is appropriate given the circumstances of the case at sentencing.

Assistance orders and the privilege against self-incrimination

70. There has been a previous assertion that assistance orders breach the privilege against self-incrimination. The Department's view is that assistance orders do not engage this privilege on the basis that an assistance order does not prevent a person from remaining silent, or compel a person to confess guilt, but allows a device to be searched. This is not dissimilar from a search warrant on a premises where access to the premises cannot be denied or frustrated on the basis of self-incrimination. Assistance orders do not compel an individual to go into their device and disclose information or documents. It simply provides an avenue for law enforcement and national security agencies to lawfully gain access to that device, so that a lawful search of the device may be conducted as necessary. Further, assistance orders must be judicially authorised.

Definition and interpretation of "material loss" or "damage"

71. The limitations and safeguards proposed for the Crimes Act and the Customs Act powers for computer access under the existing search warrant frameworks have been drafted in order to ensure that the powers are only used in an appropriate manner, proportionate to the offence being investigated.
72. Interference is permitted only where necessary to give effect to the warrant. The terms *material loss* or *damage* have not been specifically defined as doing so would unnecessarily narrow their application. Impacts that constitute loss or damage would vary considerably depending on the operational circumstances of an investigation. Given this, the intention is that these terms should be interpreted on their natural meaning, and provide means to attribute and assess loss or damage appropriately.

Schedule 5—Assistance powers for the Australian Security Intelligence Organisation

73. As a general point, the Department is continuing to consider IGIS recommendations and whether changes are appropriate.

Considering the rights of persons and ensuring persons understand their obligations under 34AAA.

74. The assistance measures are supported by robust safeguards to provide the appropriate level of oversight, and ensure requests are only issued if necessary and that protections are available for assistance provided.

75. Importantly, assistance requests are issued by Australia's highest law officer, the Attorney-General, which ensures there is appropriate oversight. The Attorney-General represents the highest-level of authority for such matters and is well equipped to consider the reasonableness and necessity of the assistance orders. The Attorney-General is also in a position to consider other factors not provided for in section 34AAA including human rights issues. For example it is entirely reasonable for the Attorney-General to reject an application for the issuance of a request on the basis that it may adversely affect human rights, unreasonably interfere with a person's privacy or impact a person that does not have the ability to understand or meet the request. Additionally, the power to make orders under section 34AAA is significantly fettered by the requirement that the Attorney-General be satisfied on reasonable grounds that the access will substantially assist the collection of intelligence as set out in 34AAA(2). It is unlikely that the Attorney-General could be satisfied of this standard if the order required ASIO to indefinitely detain and violate the rights of the specified person or otherwise harm their human dignity.

76. The powers under section 34AAA to compel a specified person to assist ASIO are not contemplated to create the basis for the deprivation of liberty or inhumane treatment. Where a specified person does not wish to comply with a section 34AAA order, this is an offence and they will have the opportunity to seek legal representation and appear before a court to have the matter heard. If an interpreter is required to communicate with the specified person, it will be in ASIO's interest as much as the individual's to obtain one as the absence of an interpreter may otherwise limit the assistance able to be offered. Information pertaining to lodging complaints against ASIO with the IGIS is freely available and the IGIS is empowered to inspect requests to the Attorney-General for assistance orders on its own motion.

77. Subsection 34AAA(4)(b) ensures that the penalties for non-compliance with an ASIO assistance order will not apply to those persons who are unable to comply.

Relationship between the powers in Schedule 1 (specifically technical assistance requests) and section 21A(1)

78. The intent and purpose of a technical assistance request (TAR) and the ASIO assistance regime are different and are not intended to be used interchangeably. TARs are part of a graduated industry assistance framework which ensures law enforcement and national security agencies can seek technical advice and assistance from 'designated communication providers' to access lawfully obtained devices and data. Failing voluntary assistance, ASIO may seek compulsory help under a TCN or TAN; these powers are designed to complement each other. To further clarify, this assistance is provided by entities across the communications supply chain and will usually be technical in nature. It is intended to help agencies adapt to technologies, like encryption, which can inhibit investigations.

Expanding the use of TARs to obtain non-technical information or assistance would be out of step with the rest of the framework which is limited by the things listed in section 317E, or things that are similar to those things.

79. Section 21A provides an assistance regime to ensure a person or body who provides reasonable and necessary assistance in relation to an ASIO function. This provision may include, but is not exclusive to, technical assistance. As a result officers may seek non-technical advice and broader documents or information that are not limited to a designated communication provider or things of a technical nature. The intent of this provision is to facilitate efforts by officers to enable persons, other than 'designated communications providers', to assist ASIO with its broader functions. It is not a part of a broader framework like TARs.

80. Safeguards and processes within the industry assistance framework have been designed to allow TARs, TANs and TCNs to operate together. To require ASIO to seek voluntary assistance outside this regime through 21A would mean that government agencies do not adopt a consistent and considered approach to industry assistance and create greater uncertainty for providers. It would also reduce the efficacy of global safeguards, like reporting requirements, which apply to all industry assistance provisions.

Proportionality and necessity of voluntary assistance orders particularly in relation to the rights of third parties and the likelihood of an order causing physical or mental harm or injury.

81. The legislative thresholds in section 21A ensures that any assistance order issued by the Director-General is founded on reasonable grounds. The Director-General represents the highest-level of authority in ASIO and is well equipped to consider the grounds of an order and considerations of reasonableness and necessity.

82. Limitations to civil immunity are clearly expressed and do not cover significant loss of, or serious damage to, property or conduct that constitutes an offence. The Department considers that these limitations are sufficiently broad to capture instances of meaningful harm to other persons.

83. The assistance regime under 21A is also voluntary in nature which means persons will not be subject to any civil penalties for non-compliance. As a result, if a person deems the requirements in an order to be unreasonable because it may cause others physical or mental harm or injury, then they are within their rights to not provide the assistance requested.

84. In the event that the operation of this section results in an acquisition of property from a person otherwise than on just terms, the Commonwealth is liable to pay a reasonable amount of compensation to the person. If the Commonwealth and the person do not agree on the amount of compensation, the person may institute proceedings in the Federal Court of Australia for the recovery from the Commonwealth of such reasonable amount of compensation as the court determines.

Relationship between voluntary assistance orders and conduct for which an ASIO warrant is required.

85. Warrants are generally intended to authorise intrusive and otherwise criminal activity. Where a warrant is required it is expected that ASIO will continue to seek the relevant permissions for the conduct in question. Proposed section 21A is voluntary and not intended as a replacement for these powers. As it cannot be used coercively and does not permit the commission of offences, the potential for overlap is limited.

86. Preventing assistance orders from being issued in circumstances where a warrant is in force is unnecessary and may create operational issues for ASIO. The intention of these measures is to ensure that ASIO can seek or receive voluntary assistance, when required, with the performance of

its function including maintaining security and fulfilling a warrant. In other words, voluntary assistance orders are not intended to allow ASIO to circumvent existing warrant regimes but to ensure that ASIO can incentivise cooperation from the community to perform its functions. Importantly, subsection 21A(1) provides clear thresholds which must be met before an assistance order can be issued.

Maximum duration for assistance requests.

Voluntary assistance requests

87. The current drafting of 21A provides flexibility for an assistance request to ensure ASIO can perform its function, and considers the potential impacts to the person and other persons. The current drafting of this provision is intended to incentivise cooperation from the person issued with an order. It also ensures that an assistance order reflects the operational environment which may demand that assistance is provided over an extended period of time or within a short time frame.
88. Subsection 21A(4) also provides scope for the Director-General and the person to enter into a contract, agreement or arrangement which may provide scope for a specified time period of compliance to be articulated. Practically speaking, it is likely that officers, on behalf of the Director-General, will engage with the person prior to the issuing of an order.
89. Providing a specified timeframe for an assistance order is also unnecessary as this power will be, in many instances, exercised in conjunction with existing ASIO warrants or other security-related operations. As a result, voluntary assistance will generally be of most utility during the life of the warrant or those operations.
90. The assistance regime under 21A is also voluntary in nature which means persons will not be subject to any civil penalties for non-compliance. As a result, if a person deems the requirements in an order to be unreasonable, they are within their right to not provide the assistance requested.

Existing oversight arrangements.

91. The IGIS has extensive powers to oversee the activities ASIO under Schedule 5 of the Bill. IGIS functions include powers to obtain information, take sworn evidence and enter agency premises.
92. Given the general extension in the oversight functions of the IGIS, the Government has announced additional funding for the IGIS. The effect of these measures on IGIS resourcing will rest on the frequency, and manner, in which the new powers may be used (as noted by the IGIS itself at the latest Senate Estimates hearings).
93. Assistance orders under section 34AAA are issued by the Attorney-General or Director-General which represents the highest-level of authority in ASIO for such matters and are well equipped to consider the reasonableness, proportionality and necessity of assistance orders.

Oral requests for assistance under section 21A.

94. The Department is comfortable with the current approach as it provides flexibility for ASIO officers to issue an assistance request in a format that is most appropriate for the operational circumstances. Subsection 21A(3) requires an orally made request for assistance to be made in writing within 48 hours. As this relates to a request made under subsection 21A(1)(a), it is appropriate to assume that the written request will be made available to the person or body it concerns. Practically speaking, it is likely that officers, on behalf of the Director-General, will engage with the person prior to the issuance of an order given the intent of section 21A which is to incentivise cooperation. This is an opportunity for officers to clarify the requirements in a request and that compliance is on a voluntary basis.

Source of power to vary, revoke or cease an assistance order.

95. The ability to vary or revoke requests under Part 15 of the *Telecommunications Act* were included in close consultation with providers. Given the ongoing, mature and frequent relationships between agencies and telecommunications industry greater form and structure was requested. Further, these ensure that TARs have consistent form and application to more compulsory powers in the framework like TANs and TCNs, each with their own variation and revocation requirements.

96. Section 21A is a more generalised power to request and receive voluntary assistance. It is intended that the Director-General's power to make a request under the proposed section 21A includes the power to revoke or vary the request. This is similar in principle to subsection 33(3) of the *Acts Interpretation Act 1901* which provides for a power to be as construed as allowing for revocation and variation in the absence of an express power to do so.

Periodic reporting requirements under section 21A and 34AAA.

97. Reporting requirements under the ASIO Act are mostly reserved for warranted activities. ASIO warrants represent one of the highest levels of authority for ASIO and permits special powers to be used in circumstances of investigating threats to Australia's security. As a result, additional levels of oversight are required to ensure these warrants are issued in the appropriate circumstances.

98. It would not be in keeping with the existing regime for the assistance orders under section 21A or 34AAA to be subjected to mandatory reporting. Mandatory reporting for assistance orders under 21A is also unnecessary considering its voluntary nature. The existing safeguards and limitations also prevents the use of assistance orders for arbitrary reasons and ensures that this power is only used in specific circumstances, explicitly limiting the potential for major loss or damage or illegal conduct.

Justification for proposed section 34AAA(2)(c)(i).

99. Given the seriousness of potential acts that are prejudicial to security, it is critical that ASIO be able to compel assistance from persons suspected of involvement. There are many ways in which involvement may be made out, but these should be viewed through the lens that there are many people with relevant knowledge that can ensure the discovery and safe resolution of activities that represent a material threat to the Australian public.

100. For example assistance can be sought from persons that are unintentionally acting as a conduit for activities that are prejudicial to security, or provide services to another person which enables them to conduct activities that are prejudicial to security. Limiting this provision to those that are knowingly and intentionally involved in activities that are prejudicial to security may inhibit legitimate ASIO investigations and intelligence gathering and establish a critical gap.

Justification for subsection 34AAA(3).

101. The safeguards in subsection 34AAA(3) are necessary as the compulsory assistance order must have regard for the fact that the premises in which the relevant computer or data storage device is located is not the premises that is specified in the warrant in force. In other words, additional oversight measures are necessary in these rare instances as the warrant relates to a different location which has not been envisaged by the issued warrant.

102. In the alternative scenario where the computer or data storage device is on premises, it is implicit that the person will provide assistance at the time of the warrant's executions and in a manner consistent with the issued warrant.

Clarifying how a compulsory assistance order under section 34AAA will be provided to a person.

103. As implicitly provided for in subsection 34AAA(4)(b), a compulsory assistance order must be provided to the specified person in a form that ensures they are able to comply with the requirements in an order.

The use of multiple coercive powers.

104. The Director-General may request that the Attorney-General make an order under section 34AAA if it is reasonable and necessary to allow the performance of specific ASIO activities. This requirement of reasonableness and necessity will go to the use of other coercive powers – if other warrants or authorisations have been issued for the same purpose and have yielded the requisite information it then follows that the relevant information or assistance will not be necessary.

105. The IGIS is able to investigate the use of compulsory assistance orders under their existing oversight powers, including their use in conjunction with other ASIO powers. The Department will work with IGIS to determine if further amendments are required to facilitate their ongoing oversight function.