3

Monitoring of persons subject to control orders

3.1 This chapter discusses the following provisions of the Bill, which primarily relate to the monitoring of persons subject to control orders in operation:

- Schedule 3 amends the Criminal Code to place obligations on a person who is required to wear a tracking device under a control order to ensure that the device remains operational and functional.
- Schedule 8 creates a new monitoring powers regime under the *Crimes Act 1914* (the Crimes Act) for entering premises or searching persons in order to monitor the compliance of a person who is subject to a control order with the conditions of their control order, and for preventing such a person from engaging in a terrorist act or planning or preparatory acts.
- Schedule 9 amends the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to
  - ⇒ allow agencies to apply for a Telecommunications Interception (TI) warrant for the purposes of monitoring compliance with a control order,
  - ⇒ allow TI information to be used in any proceedings associated with that control order, and
  - ⇒ permit the use of intercepted material in connection with preventative detention orders (PDOs) nationally.
- Schedule 10 amends the *Surveillance Devices Act 2004* (the SD Act) to
  - ⇒ allow law enforcement officers to apply for a surveillance device warrant for the purposes of monitoring compliance with a control order,

- ⇒ allow that information to be used in any proceedings associated with that control order,
- ⇒ extend the circumstances in which agencies can use less intrusive surveillance devices without a warrant to include monitoring of compliance with a control order, and
- ⇒ allow protected information obtained under a control order warrant to be used to determine whether the control order has been complied with.

Tracking devices (Schedule 3)

3.2 One of the obligations that may be placed on a person subject to a control order is to require the person to wear a tracking device.[1] A tracking device used in association with a control order is a small, portable device used to monitor a person's location. It is worn on the body of the person, often around the ankle, and is used to locate and track a person's movements. Similar tracking devices are sometimes used to monitor individuals released on bail or parole to ensure compliance with bail or parole conditions, which often include curfews or prohibitions on entering or approaching particular locations.

3.3 Schedule 3 to the Bill proposes to amend the Criminal Code to require a person subject to such a requirement to take steps, to be set out in the control order, to ensure the tracking device remains operational and functional. Specifically, the person would be required to

> (a) take specified steps and reasonable steps to ensure that the tracking device and any equipment necessary for the operation of the tracking device are or remain in good working order;
>
> (b) authorise one or more AFP members to take specified steps to ensure that the tracking device and any equipment necessary for the operation of the tracking device are or remain in good working order;
>
> (c) authorise one or more AFP members to enter one or more specified premises for the purposes of installing any equipment necessary for the operation of the tracking device;
>
> (d) report to specified persons at specified times and places for the purposes of having the tracking device inspected;

1 *Criminal Code Act 1995* (Criminal Code), paragraph 104.5(3)(d).

> (e) if the person becomes aware that the tracking device or any equipment necessary for the operation of the tracking device is not in good working order—notify an AFP member as soon as practicable, but no later than 4 hours, after becoming so aware.[2]

3.4 The Explanatory Memorandum notes that there are no obligations under the current control order regime for the person to keep their tracking device charged and operational. The amendments are thus intended to 'ensure the utility of a requirement to wear a tracking device':

> Requiring a person who is required to wear a tracking device to take steps to ensure that the device is charged and operational is necessary to prevent the effective operation of the requirement from being frustrated without technically breaching the requirements of the control order, which carries a criminal penalty. Ensuring the effective operation of a requirement to wear a tracking device is designed to support compliance with other related conditions, such as restrictions on movement.[3]

Matters raised in evidence

3.5 The Attorney-General's Department explained in its submission that

> [t]he steps that the AFP will be able to request and an issuing court will be able to impose, will include 'specified' steps to ensure the tracking device is or remains in good working order (for example, by agreeing to answer the phone if the AFP call because the device appears not to be working) and take 'reasonable' steps to ensure the device remains in good working order (for example, regular charging of the device).
>
> The amendments do not give an issuing court a discretion to impose the additional obligations in relation to maintaining the operation of the device. That is, the issuing court can either impose the requirement to wear a tracking device and the accompanying requirements to maintain the device or neither requirement. The rationale for this is that a requirement to wear a device without the accompanying requirements would be ineffective.[4]

3.6 Several submitters raised concerns with these provisions. Common themes were that the proposed provisions inappropriately place responsibilities on persons who are the subject of control orders, rather

2 Proposed subsection 104.5(3A).

3 Explanatory Memorandum, p. 57.

4 Attorney-General's Department, *Submission 9*, pp. 5–6.

than police, and a lack of clarity as to what the provisions actually require.[5]

3.7 The Law Council of Australia considered the requirement to take 'reasonable steps', in addition to 'specified steps', could create confusion as to what was actually required to be done as there may be different views about what are considered to be 'reasonable steps'. It raised the example of a faulty battery, in relation to which it suggested a person may not know whether they have an obligation to fix the battery or simply to report the matter to the AFP.[6]

3.8 The Council noted that a breach of a control order may attract criminal liability, and that the rule of law requires that a person 'know in advance whether their conduct might attract a criminal sanction.'[7] It recommended that the requirement to take 'reasonable steps' be removed, as the 'specified steps' requirement would allow an issuing authority to tailor the control order to the specific circumstances of the subject of the control order. Further, it recommended that the subject of the control order should not be required to authorise AFP members to take specified steps to ensure the device is in good working order or to enter premises, as such actions should be authorised by the court.[8]

3.9 The Gilbert + Tobin Centre of Public Law made a similar argument, contending 'it should be the responsibility of the police to ensure the technology is in good working order.'[9] It suggested that if the legislation is seeking to address concerns about the disabling of tracking devices, this should be addressed 'by a clear prohibition of interference with the device.'[10]

3.10 Submitters were particularly concerned as to how the responsibility of ensuring the functioning of a tracking device would apply to children.

3.11 The Muslim Legal Network (NSW) questioned the ability of minors to assess whether a tracking device is defective and whether a report to the AFP would need to be made.[11] It also submitted that it would be 'onerous

5 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 6; Law Council of Australia, *Submission 6*, p. 14; Muslim Legal Network (NSW), *Submission 11,* p. 12.

6 Law Council of Australia, *Submission 6*, p. 14.

7 Law Council of Australia, *Submission 6*, p. 14.

8 Law Council of Australia, *Submission 6*, p. 14.

9 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 6.

10 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 6.

11 Muslim Legal Network (NSW), Submission 11, p. 12.

and impractical' to transfer this responsibility to a parent or guardian of the child.[12]

3.12 In a similar vein, the Queensland Government suggested that

> young people may be more likely to negligently damage or fail to maintain equipment due to their developmental life stage. This could be relevant in relation to a young person's failure to charge a device, when a particularly immature 14 year old may not understand (or remember) the significance of ensuring this simple action occurs (and by failing to do so, they may be committing a criminal offence).[13]

3.13 Accordingly, the Queensland Government submitted the proposed mandatory conditions should not apply in cases where a court imposes a condition on a young person to wear a tracking device.[14]

3.14 As with a range of other provisions proposed by the Bill, the Muslim Legal Network (NSW) commented that proposed subsection 104.5(3A) could provide AFP officers 'with the ability to enter into various premises, including perhaps a school'.[15] It submitted there is 'no doubt' this would impact upon the mental wellbeing of the subject of the control order, as well as other aspects of their life.[16]

3.15 In its supplementary submission, the Attorney-General's Department responded to these concerns, noting that

> [a]n issuing court will only impose as a condition of the order that the young person wear a tracking device if it determines on a balance of probabilities that the restriction is reasonably necessary, and reasonably appropriate and adapted for the purposes of protecting the public from a terrorist attack, preventing the provision of support for or the facilitation of a terrorist attack or preventing the provision of support for or the facilitation of the engagement in a hostile activity in a foreign country. When determining what is 'reasonably necessary, and reasonably appropriate and adapted', the issuing authority must consider the impact of the tracking device (including the mandatory conditions associated with the device, such as maintaining it in good working order) on the young person's circumstances and consider the best

12 Muslim Legal Network (NSW), *Submission 11*, p. 12.

13 Queensland Government, *Submission 16*, p. 2.

14 Queensland Government, *Submission 16*, p. 3.

15 Muslim Legal Network (NSW), *Submission 11*, p. 12.

16 Muslim Legal Network (NSW), *Submission 11,* p. 12.

> interests of the young person, for example their maturity, lifestyle, and right to receive education …
>
> A tracking device which has run out of battery will render a requirement to wear a tracking device ineffective, but may not constitute interference with the device. Consequently, it is important that the Bill provides the ability to prosecute a person in circumstances where they not only interfere with the device but intentionally render it ineffective by letting it run out of battery.
>
> Any prosecution for an offence must be supported by admissible evidence and both the physical and fault elements proved to the criminal standard beyond reasonable doubt.[17]

Committee comment

3.16 The Committee notes submitters' concerns that Schedule 3 as proposed is ambiguous in some respects, namely the requirements to take 'reasonable steps' and to authorise AFP members to take specified steps to ensure the device is in good working order or to enter premises. The Committee considers that these issues should be clarified. This should include a non-exhaustive list of examples in the Explanatory Memorandum of what would be expected to constitute 'reasonable steps'. The Bill should also make it clear that it is the court making the order, rather than the person subject to the order, who authorises the AFP to take specified steps to ensure the device remains in good working order and to enter specified premises to install necessary equipment.

3.17 With respect to the deliberate disabling of a tracking device, the Bill should be amended to include a clear prohibition on interference with the device. The inclusion of this amendment, in addition to the proposed requirements already set out in Schedule 3, would ensure that the full range of actions or inactions which would render a tracking device inoperative are captured by the Bill.

3.18 In relation to the application of the proposed obligations on a child who is required to wear a tracking device under a control order, the Committee considers this appropriate, noting that:

- the ability of a child to understand the terms of a control order may vary depending on their individual development and maturity, which would be considered by an issuing court in deciding whether or not to impose a requirement to wear a tracking device, and

17 Attorney-General's Department, *Submission 9.1*, p. 14.

- the court must take into account the best interests of the child in determining whether to include a requirement to wear a tracking device as part of a control order placed on a child, including the mental health of the child.

3.19 The Committee notes that, as with other criminal offences, the prosecution must prove an offence of contravening a control order beyond reasonable doubt. That is, the prosecution would be required to lead evidence as to the individual's state of mind, including their subjective intention or knowledge that their actions would result in, or be likely to result in, a breach of the control order. It would not be enough to show that the individual should have known that their actions would result in a breach.

3.20 In light of these points, the Committee considers that the risk of a person, including a child, being prosecuted for breaching the additional obligations in relation to wearing a tracking device will be appropriately confined to cases of flagrant and egregious breaches. In the case of a child, the maturity of the child and their developmental stage would be key factors not only in determining whether to impose a requirement to wear a tracking device, but also in determining whether prosecution for a breach of a tracking device requirement is justified.

Recommendation 8

The Committee recommends that, in regard to the obligations to be imposed on a person required to wear a tracking device under a control order, the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 be amended to:

- **remove the ambiguity in subparagraphs (3A)(b) and (c) in Schedule 3 to clarify that it is the court, not the subject of the control order, which authorises any 'specified steps' to be taken by the Australian Federal Police to ensure the device remains in good working order and to enter specified premises to install necessary equipment, and**
- **include a clear prohibition on interfering with a tracking device that is required to be worn by the subject of a control order, in addition to the other requirements set out in Schedule 3 of the Bill.**

The Committee also recommends that the Explanatory Memorandum be amended to include examples of what would constitute reasonable steps to ensure the device remains in good working order.

Monitoring powers (Schedule 8)

3.21 Schedule 8 to the Bill proposes to amend the Crimes Act by inserting a new Part 1AAB granting the power to police to enter premises or search persons, and to exercise other 'monitoring powers', in order to monitor the compliance of individuals subject to a control order with the controls in the order.

Powers in relation to premises

3.22 Under proposed section 3ZZKA, police would be able to enter premises and exercise the monitoring powers if a control order is in force in relation to a person and the person has a 'prescribed connection' with the premises,[18] and:

- the person is the occupier of the premises and consents to the entry, or

18 Proposed section 3ZZJC sets out when a person will have a 'prescribed connection' with premises.

- the entry is made under a monitoring warrant, and
- the entry and exercise of monitoring powers are for any of the following purposes (the control order monitoring purposes):
  - ⇒ the protection of the public from a terrorist act;
  - ⇒ preventing the provision of support for, or the facilitation of, a terrorist act;
  - ⇒ preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
  - ⇒ determining whether the control order has been, or is being, complied with.

3.23 The first three of the control order monitoring purposes mirror the purposes for which a control order can be made under section 104.1 of the Criminal Code. The fourth is specific to the monitoring powers in the Bill.

3.24 The monitoring powers that would be able to be exercised in relation to the premises are set out in proposed sections 3ZZKB, 3ZZKC and 3ZZKD. These powers are:

- the power to search the premises and any thing on the premises,
- the power to search for and record fingerprints found at the premises,
- the power to take samples of things found at the premises,
- the power to examine or observe any activity conducted on the premises,
- the power to inspect, examine, take measurements of or conduct tests on any thing on the premises,
- the power to make any still or moving image or any recording of the premises or any thing on the premises,
- the power to inspect any documents on the premises,
- the power to take extracts from, or make copies of, any such document,
- the power to take onto the premises equipment and materials required for the purpose of exercising powers in relation to the premises,
- the power to operate electronic equipment on the premises and to use tapes, disks or other storage devices that are on the premises and can be used with it, and
- if 'relevant data' is found in the exercise of the monitoring powers, the power to operate electronic equipment to:

- ⇒ put the data in documentary form and remove the documents from the premises,
- ⇒ transfer the data onto a disk, tape or other storage device and remove the disk, tape or other storage device from the premises.

3.25 Where premises are entered under a monitoring warrant only, police would have the power to secure any electronic equipment on the premises to obtain expert assistance. This power would be able to be exercised if it is suspected on reasonable grounds that relevant data may be accessible by operating the equipment, expert assistance is required to do so and, in the absence of the equipment being secured, the relevant data may be destroyed, altered or otherwise interfered with.[19]

3.26 Proposed section 3ZZKE would provide additional powers to ask questions or seek the production of documents, with the precise nature of the power depending on whether premises have been entered under a monitoring warrant or on the basis of consent. Where premises have been entered on a consensual basis, police would have the power to ask questions of the occupier and request the occupier to produce any document that is likely to assist with the control order monitoring purposes.[20] However, in such circumstances, there is no requirement for the occupier to answer questions or produce documents.

3.27 Where premises have been entered under a monitoring warrant, police would have the power to require *any* person on the premises to answer questions or produce any document that is likely to assist with the control order monitoring purposes.[21] However, the person is not required to answer questions or produce any document if the person does not possess the information or document required and has taken all reasonable steps available to the person to obtain the information or document.[22] The person is not required produce a document if the document is not at the premises.[23] Failure to comply with a requirement to answer questions or produce documents would constitute an offence.[24]

3.28 In addition, only where premises are entered on the basis of a monitoring warrant, police would have the power to:

- seize evidential material and other things found during the exercise of monitoring powers (if certain criteria are met, as discussed below), and

19 Proposed section 3ZZKD.

20 Proposed subsection 3ZZKE(2).

21 Proposed subsection 3ZZKE(3).

22 Proposed subsection 3ZZKE(4).

23 Proposed subsection 3ZZKE(5).

24 Proposed subsection 3ZZKE(6).

- conduct an ordinary search or a frisk search of a person at or near the premises if it is suspected on reasonable grounds that the person has any evidential material or seizable items in their possession.[25]

3.29 Proposed section 3ZZKG would provide police with the power to use such force as is necessary and reasonable against persons and things in executing a monitoring warrant in relation to premises and in exercising the seizure powers under proposed section 3ZZKF.

The power to search persons

3.30 Under proposed section 3ZZLA, police would be able to conduct an ordinary search or a frisk search of a person if a control order is in force in relation to a person and:

- the person has consented to the search, or
- the search is conducted under a monitoring warrant, and
- the search is for one of the control order monitoring purposes.

3.31 The monitoring powers that would be able to be exercised in relation to the person are set out in proposed section 3ZZLB. These powers are:

- the power to search things found in the possession of the person,
- the power to search any recently used conveyance (e.g. a vehicle), and
- the power to record fingerprints or take samples from things found in the course of a search of the person, of things in their possession or in any recently used conveyance.

3.32 In addition, under proposed section 3ZZLC, where a search is conducted on the basis of a warrant—but not in the case of a consensual search—police would have certain seizure powers, which are discussed below.

3.33 Proposed section 3ZZKG, which provides police with powers to use force when executing a monitoring warrant in relation to premises and exercising seizure powers, is mirrored by proposed section 3ZZLD, in relation to the execution of monitoring warrants in relation to persons.

Seizure powers

3.34 Under the proposed provisions, where premises are entered or a person is searched under a monitoring warrant, police would also have powers to seize certain things. Specifically, police would have the power to seize:

25 Proposed section 3ZZKF.

- evidential material (as defined in Part 1AA of the Crimes Act)[26] found:
  - ⇒ in the course of the exercise of monitoring powers on the premises, or
  - ⇒ in the course of the search of the person or recently used conveyance, and
- other things:
  - ⇒ found during the exercise of monitoring powers on the premises, or
  - ⇒ on or in the possession of the person or in the recently used conveyance

  that police believe on reasonable grounds to be:
  - ⇒ evidential material (within the meaning of the *Proceeds of Crimes Act 2002*),[27]
  - ⇒ tainted property (within the meaning of the *Proceeds of Crimes Act 2002*),[28] or
  - ⇒ seizable items.[29]

Applications for monitoring warrants

3.35 The application process for monitoring warrants in relation to premises and persons are set out at proposed sections 3ZZOA and 3ZZOB respectively. These provisions also set out the requirements for the contents of warrants issued.

3.36 Under proposed section 3ZZOA, an application would need to be made to an issuing officer (a magistrate acting in their personal capacity), who may issue a monitoring warrant in relation to premises if satisfied a control order is in force in relation to a person, the person has a prescribed connection with the premises and, having regard to a number of specified matters, it is reasonably necessary that police have access to the premises for a control order monitoring purpose.

---

26 Section 3C of the Crimes Act provides that 'evidential material' means 'a thing relevant to an indictable offence or a thing relevant to a summary offence, including such a thing in electronic form'.

27 Under section 338 of the *Proceeds of Crime Act 2002*, 'evidential material' means evidence relating to: (a) property in respect of which action has been or could be taken under that Act; (b) benefits derived from the commission of an indictable offence, a foreign indictable offence or an indictable offence of Commonwealth concern; or (c) literary proceeds.

28 Under section 338 of the *Proceeds of Crime Act 2002,* 'tainted property' means: (a) proceeds of an indictable offence, a foreign indictable offence or an indictable offence of Commonwealth concern; or (b) an instrument of an indictable offence.

29 'Seizable item' is defined in section 3C of the Crimes Act as 'anything that would present a danger to a person or that could be used to assist a person to escape from lawful custody'.

3.37 Under proposed section 3ZZOB, the issuing officer would be able to issue a monitoring warrant in relation to a person if satisfied a control order is in force in relation to the person and, having regard to a number of specified matters, it is reasonably necessary that police should conduct an ordinary search or a frisk search of the person for a control order monitoring purpose.

3.38 The matters the issuing officer must have regard to when considering an application for a monitoring warrant in relation to a premises or person include the possibility that the subject of the control order has or will engage in conduct connected to the control order monitoring purposes.[30] When considering issuing a monitoring warrant in respect of premises, the issuing officer must also have regard to the nature of the person's prescribed connection with the premises.[31]

3.39 In the event that a monitoring warrant is issued on the basis that a control order is in force and:

- the control order is revoked,
- the control order is declared to be void, or
- a court varies the control order by removing one or more obligations, prohibitions or restrictions imposed by the control order,

proposed section 3ZZOD provides that the monitoring warrant must not be executed and any consequential powers must not be exercised.

Other provisions

3.40 Proposed Part 1AAB would require police to comply with certain obligations when entering premises or searching persons under the monitoring powers regime, including obligations in relation to seeking the consent of an occupier to enter premises or of a person to search them, and that the person must be notified that they may refuse consent.[32] When exercising powers under a monitoring warrant, obligations include that the officer must be in possession of the warrant (or a copy) and to give the occupier a copy of the warrant.[33]

3.41 The provisions would also require the Commonwealth to provide compensation for damage to electronic equipment incurred as a result of the equipment being operated in the exercise of monitoring powers, entitle

30 Proposed subsections 3ZZOA(4) and 3ZZOB(4).

31 Proposed subparagraph 3ZZOA(2)(c)(i).

32 Proposed section 3ZZNA.

33 Proposed sections 3ZZND and 3ZZNE.

occupiers to be present during a search of their premises and entitle a person who is subject to a control order to be present and observe a search of premises under a monitoring warrant.[34]

3.42 Proposed sections 3ZZRA to D relate to things seized, documents produced and answers given as a result of the exercise of monitoring powers. As noted in the Explanatory Memorandum, proposed section 3ZZRB would provide that existing provisions in Division 4C of Part 1AA of the Crimes Act would apply to things seized under the monitoring powers. The applied provisions specify:

> the purposes for which things and documents may be used and shared by a constable or Commonwealth officer, the requirements for operating seized electronic equipment, compensation for damaged electronic equipment, and the requirements for returning things seized or documents produced.[35]

3.43 The provisions of Division 4C of Part 1AA of the Crimes Act would similarly apply to documents produced under the monitoring powers, by virtue of proposed subsection 3ZZRC(1). Documents produced under the monitoring powers would also be able to be used for the control order monitoring purposes.[36]

3.44 Information provided in response to questions asked under the monitoring powers would only be able to be used for the control order monitoring purposes and the additional purpose of preventing, investigating or prosecuting an offence.[37]

3.45 Where the interim control order providing the basis for the use of monitoring powers has been declared void by a court, things seized, information obtained or documents produced under monitoring powers while the interim control order was in force would be able to be adduced as evidence, used or communicated for limited purposes. The thing, information or document could only be adduced, used or communicated by a person if the person reasonably believes that doing so is necessary to assist in preventing, or reducing the risk of, the commission of a terrorist act, serious harm to a person or serious damage to property, or for purposes connected with PDOs under Commonwealth, State or Territory laws.[38]

34 Proposed sections 3ZZNF, 3ZZNG and 3ZZNH.

35 Explanatory Memorandum, p. 80.

36 Proposed subsection 3ZZRC(2).

37 Proposed paragraph 3ZZRD(e).

38 Proposed section 3ZZTC.

Matters raised in evidence

3.46 The proposed monitoring powers regime was the subject of several submissions. Key concerns were the threshold for the issue of a monitoring warrant and the effect of the monitoring powers on the privacy of the subject of the control order and third parties.

3.47 Several submitters expressed concern that the proposed threshold for the issue of a monitoring warrant is too low.[39] Comments focused on the ability of an issuing officer to issue a monitoring warrant on the basis of the 'possibility' that the subject of the control order has contravened, is contravening, or will contravene the control order.[40] According to the Australian Human Rights Commission:

> The new warrant powers that the Bill would introduce are different from other warrant powers, in that an issuing authority would not need to be satisfied that there is reason to suspect a person may have breached a control order or committed any other offence.[41]

3.48 Similarly, the Muslim Legal Network (NSW) submitted

> the monitoring warrant regime also lowers significantly the threshold for the application of said warrant. The Muslim Legal Network (NSW) submits that the proposed threshold is far too low …[42]

3.49 Amongst such submissions, there appeared to be a consistent view that if the proposed monitoring regime were to be retained, the threshold for the issuing of a monitoring warrant should at least require a suspicion that the control order was being breached.[43] For example, the Gilbert + Tobin Centre of Public Law suggested that a magistrate should be authorised to issue a monitoring warrant only where a police officer suspects on reasonable grounds that the person is failing to comply with an order.[44]

3.50 Many submitters also raised the impacts of the monitoring powers on the privacy and human rights of the subject of the control order and of third

39 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 10; Australian Human Rights Commission, *Submission 5*, pp. 17–18; Law Council of Australia, *Submission 6*, pp. 16–17, p. 21; Muslim Legal Network (NSW), *Submission 11*, p. 27; Joint councils for civil liberties, *Submission 17*, p. 14.

40 Proposed paragraphs 3ZZOA(4)(f), 3ZZOB(4)(f).

41 Australian Human Rights Commission, *Submission 5*, pp. 17–18.

42 Muslim Legal Network (NSW), *Submission 11*, p. 27.

43 See Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 10; Australian Human Rights Commission, *Submission 5*, p. 18; Law Council of Australia, *Submission 6*, p. 21.

44 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 10.

parties.[45] In particular, submitters expressed concerns regarding the breadth of powers available under a monitoring warrant, and the wide range of premises that could be subject to a monitoring warrant by virtue of having a 'prescribed connection' to the subject of a control order. Concerns were also raised in relation to the use of information and evidence obtained under the monitoring powers.

3.51 Australian Lawyers for Human Rights submitted:

> We are concerned that the **degree of monitoring** of a person who is subject to a control order is, under the proposed amendments, **virtually unlimited** and capable of stripping that person of all privacy and such basic rights as the rights to privacy, to liberty, to freedom of speech, of assembly, of movement and of security.[46]

3.52 The Muslim Legal Network (NSW) questioned the breadth and purpose of the monitoring warrant regime, asserting that:

> As a starting proposition, it is disingenuous to submit in the proposed bill that the simplified outline is limited to what is described below when it is clear that the insertion of Part 1AAB seeks more than simply an exercise in 'monitoring compliance of control orders'. It is clearly designed to operate as an investigative extension of the control order provisions.[47]

3.53 The Independent National Security Legislation Monitor alluded to similar concerns in the context of his report on the desirability of including provisions for special advocates within the Bill:

> The details of the potential monitoring blur, if not eliminate, the line between monitoring and investigation … The significance for present purposes is to emphasise the seriousness of the impact upon a person of the grant of a control order if these changes come into force and the consequent necessity for proper safeguards of the interests of a potential controlee.[48]

45 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 10; Australian Lawyers for Human Rights, *Submission 4*, p. 4; Australian Human Rights Commission, *Submission 5*, pp. 17–18 and *Supplementary Submission 5.1*, p. 1; Law Council of Australia, *Submission 6*, pp. 16–17, p. 21; Muslim Legal Network (NSW), *Submission 11*, p. 27; Joint councils for civil liberties, *Submission 17*, pp. 14–15.

46 Australian Lawyers for Human Rights, *Submission 4*, p. 4. Emphasis in the original.

47 Muslim Legal Network (NSW), *Submission 11*, p. 24.

48 The Hon Roger Gyles AO QC, Independent National Security Legislation Monitor, *Control order safeguards – (INSLM report) special advocates and the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015*, January 2016, p. 3.

3.54 The joint civil liberties councils queried whether existing monitoring and surveillance powers were in fact insufficient to allow effective, legitimate monitoring of persons subject to a control order.[49] However, they suggested that the proposed powers might be more defensible if they were limited to the objective of the legislation to prevent terrorism:

> There may be greater justification for a blanket authority to monitor persons who have a control order if the purpose was indeed restricted to reducing 'the risk that a person will engage in terrorist act planning or preparatory acts while subject to a control order'.[50]

3.55 The Gilbert + Tobin Centre of Public Law argued that the low threshold for the issue of a monitoring warrant, where the magistrate is satisfied that it is reasonably necessary for the purposes of determining whether the control order has been, or is being complied with, would provide a 'blanket authorisation for police officers to conduct searches for the purpose of monitoring whether a person is complying with an order.'[51] It highlighted the range of powers authorised under a monitoring warrant, including powers to conduct a frisk search of a person, take fingerprints, take samples and photographs, seize evidentiary material, make copies of documents and use electronic equipment to record relevant data, and ask questions and seek production of documents.[52]

3.56 In light of the breadth of these monitoring powers, Gilbert + Tobin suggested the control order regime may be rendered vulnerable to constitutional challenge. It noted that the High Court of Australia upheld the constitutionality of the control order regime in *Thomas v Mowbray* (2007) 233 CLR 307, in part based on its view that control orders were not punitive measures.[53] At the public hearing, Professor Andrew Lynch from Gilbert + Tobin stated that

> in overlaying new processes to monitor compliance with control orders, [the Gilbert + Tobin Centre of Public Law] suggest the bill alters the orders in a way that moves them closer to a punitive measure and so may risk unconstitutionality.[54]

3.57 However, Professor Lynch qualified this point later in the hearing, stating

49 Joint councils for civil liberties, *Submission 17*, p. 13.

50 Joint councils for civil liberties, *Submission 17*, p. 13.

51 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 9.

52 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 10.

53 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 10.

54 Professor Andrew Lynch, Gilbert + Tobin Centre of Public Law, *Committee Hansard*, Canberra, 14 December 2015, p. 18.

> there is a case to be made for monitoring compliance with the control order. If the control orders are going to remain as part of the national security framework, then they should be as effective as possible. The experience in the UK of people absconding on control orders is an instructive one, and is something to be avoided …
>
> It may well be that there is nothing in the prospect that we raise, but we think it is a prospect because you are actually adding a second layer or a second tier to the existing scheme which is being upheld.[55]

3.58 The joint civil liberties councils raised specific concerns regarding the powers to operate electronic equipment, noting the large amount of personal information likely to be stored on electronic devices. It submitted that, in conjunction with the types of premises with which a person could have a 'prescribed connection', the exercise of powers to operate electronic equipment could potentially intrude on the right to privacy of innocent third party persons.[56]

3.59 The Muslim Legal Network (NSW) and the Law Council of Australia separately raised concerns regarding the impact on the privacy of the subject of the control order and third parties of the power to require a person on a premises entered under a monitoring warrant to answer any questions, and produce any documents, that are likely to assist in any of the purposes for which a monitoring warrant may be issued.[57]

3.60 The Muslim Legal Network (NSW) stated that:

> Whilst 3ZZJD provides a limited protection against self-incrimination, 3ZZKE is open to abuse and infringement of an individual's right to silence where they may not be instructed in such a respect or have available to them the assistance of a legal practitioner. This is particularly intrusive in circumstances where a person in attendance at a relevant premises may have no contact with the individual subject to a control order.[58]

3.61 Similarly, the Law Council of Australia submitted that the power 'purports to conscript other persons present to assist with the investigation being undertaken under pain of punishment'.[59] The Council

55 Professor Andrew Lynch, Gilbert + Tobin Centre of Public Law, *Committee Hansard*, Canberra, 14 December 2015, p. 22.

56 Joint councils for civil liberties, *Submission 17*, pp. 14–15.

57 Proposed subsections 3ZZKE(3)–(6).

58 Muslim Legal Network (NSW), *Submission 11*, pp. 25–26.

59 Law Council of Australia, *Submission 6*, p. 17.

submitted that answers given under compulsion could be used to further an investigation or prosecution as proposed paragraph 3ZZRD(e) provides 'no limitation or definition as to "prosecuting an offence"'.[60]

3.62 The Law Council of Australia also opposed the inclusion of the following incidental powers that may be exercised by a constable executing a monitoring warrant:[61]

- proposed paragraph 3ZZKF(2)(b)—the power to seize other things found during the exercise of monitoring powers on a premises searched under monitoring warrant if the constable believes on reasonable grounds that the things are evidential material or tainted property, within the meaning of the *Proceeds of Crime Act 2002*; and
- proposed subsection 3ZZLC(2)—in relation to the search of a person or recently used conveyance under a monitoring warrant, the power to:
  - ⇒ seize evidential material[62] found in the course of the search;
  - ⇒ seize things the constable believes on reasonable grounds to be evidential material or tainted property within the meaning of the *Proceeds of Crime Act 2002*; and
  - ⇒ seize other things the constable believes on reasonable grounds to be seizable items.[63]

3.63 The Council submitted that these incidental powers are not necessary for the purposes of the legislation to be realised as '[t]here is already a power to seize information in relation to preventing the support for or the facilitation of a terrorist act', and noted that the *Proceeds of Crime Act 2002* has quite different objects to the proposed legislation.[64]

3.64 The ability to use in proceedings information obtained under a monitoring warrant where the grounds on which it was issued no longer exist (e.g. the control order as it was originally issued is no longer in force) was also raised as an issue.

3.65 The Law Council of Australia submitted that under proposed subsections 3ZZOD(2) to (4), a thing, a document or information may be admissible in

60 Law Council of Australia, *Submission 6*, p. 17.

61 Law Council of Australia, *Submission 6*, p. 17.

62 'Evidential material' has the same meaning as in Part 1AA of the *Crimes Act 1914* (Cth), which is defined in subsection 3C(1) of that Act as 'a thing relevant to an indictable offence or a thing relevant to a summary offence, including such a thing in electronic form'.

63 'Seizable item' has the same meaning as in Part 1AA of the *Crimes Act 1914* (Cth), which is defined in subsection 3C(1) of that Act as 'anything that would present a danger to a person or that could be used to assist a person to escape from lawful custody'.

64 Law Council of Australia, *Submission 6*, p. 17.

civil proceedings, including proceedings under the *Proceeds of Crime Act 2002*k, even if obtained in breach of the requirement not to execute a monitoring warrant if the control order is revoked, declared void, or varied by the removal of one or more obligations, prohibitions or restrictions.[65] The Council opposed the admissibility of such evidence in such proceedings, due to the difference in objectives from the proposed legislation.[66]

3.66 The Muslim Legal Network (NSW) submitted that proposed section 3ZZTC, would provide an exemption for evidence obtained improperly or illegally, as it would allow a thing, information or document obtained under a monitoring warrant executed before a control order is subsequently declared void to be adduced in proceedings. It submitted:

> Clearly, this is in contradiction with principles espoused in s. 138 of the Evidence Act.[67]

3.67 To mitigate these impacts on privacy, submitters made a range of suggestions to amend the monitoring powers regime. The Australian Human Rights Commission recommended that monitoring warrants only be granted 'where the relevant authority is satisfied that there are no less intrusive means of obtaining the information'.[68] The Gilbert + Tobin Centre of Public Law submitted that the definition of 'prescribed connection' to a premises triggering a monitoring warrant to search premises should be narrowed.[69]

3.68 The Law Council of Australia recommended that:

- the privileges that are not abrogated (referring to the privileges of self-incrimination and legal professional privilege, as set out in proposed section 3ZZJD) should be clearly stated in any notice given of the monitoring powers being exercised,[70]
- proposed subsections 3ZZKE(3)–(6) regarding the power to require the answering of questions and production of documents not be passed,[71] and

65 Law Council of Australia, *Submission 6*, p. 20.
66 Law Council of Australia, *Submission 6*, p. 20.
67 Muslim Legal Network, *Submission 11*, p. 26.
68 Australian Human Rights Commission, *Submission 5*, p. 18.
69 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 10.
70 Law Council of Australia, *Submission 6*, p. 17.
71 Law Council of Australia, *Submission 6*, p. 17.

- the Committee inquire into whether the power to issue a monitoring warrant is delegable and whether it would be more appropriate for the issuing officer for a monitoring warrant to be a Supreme Court judge.[72]

3.69 The Queensland Government submitted that Schedule 8 should be amended to incorporate an oversight and reporting role for the Queensland Public Interest Monitor (PIM). This would then require an issuing authority considering the issue of a monitoring warrant to an agency in Queensland to have regard to any submissions made by the Queensland PIM.[73]

3.70 The AFP submission outlined the importance of being able to monitor and enforce compliance with a control order to ensure its effectiveness. The AFP submitted that

> a control order is only as effective as the ability of police to monitor and enforce the subject's compliance with the conditions imposed by the control order. While the imposition of a control order may in itself be sufficient to deter some individuals from engaging in the behaviours or activities restricted under the order, in some cases, individuals have attempted to subvert their conditions …
>
> As with any laws restricting the freedom of persons to engage in specified conduct, the legal and practical ability of authorities to monitor and enforce compliance is a key factor in promoting voluntary compliance amongst the population. Law enforcement is restricted in its ability to monitor and enforce compliance with control orders both by operational resourcing, and gaps in the drafting of laws.[74]

3.71 Similarly, in its supplementary submission, the Department referred to comments made by the former Independent National Security Legislation Monitor (INSLM) that a control order itself is unlikely to have a significant deterrent effect on someone intent on causing harm through terrorist activity.[75] It submitted:

72 Law Council of Australia, *Submission 6*, p. 17.

73 Queensland Government, *Submission 16*, p. 4. Noting the requirement that the Queensland Public Interest Monitor report annually with respect to control orders, the Queensland Government recommended that the provisions be amended to provide for deferred public reporting by the Queensland PIM on the use of monitoring warrants.

74 Australian Federal Police, *Submission 3*, pp. 9–10.

75 Independent National Security Legislation Monitor, *Declassified Annual Report*, December 2012, Chapter II, as cited in Attorney-General's Department, *Submission 9.1*, p. 18.

> Enabling agencies to monitor a person's compliance with a control order is likely to increase the deterrence element, as the controlee will be aware that their behaviour can be more readily monitored. This is likely to enhance the preventative effect of control orders and increase their effectiveness in protecting the public from a terrorist act.[76]

3.72 For this reason, the AFP stated that it is 'imperative that law enforcement has adequate powers to monitor a person's compliance with the conditions of the control order' and submitted that current provisions do not confer such powers.[77] Assistant Commissioner Neil Gaughan stated at the public hearing:

> That is a significant gap for us at the moment. Even though we have an order saying 'X', we actually cannot monitor that.[78]

3.73 The AFP submission further noted that it is currently not able to apply for a search warrant, TI warrant or surveillance device warrant until and unless it is suspected that an offence has already occurred.[79]

3.74 The Attorney-General's Department noted the implications of only being able to apply for a warrant after it is suspected that an offence has already occurred:

> Given the gravity of the purposes for which a control order is made, compliance with its terms is clearly important. If compliance could only be monitored once there was information that a breach had occurred, the damage would have been done and lives may have been lost.[80]

3.75 Addressing concerns raised by submitters regarding the threshold for issue of monitoring warrants, the Department noted that

> in order to apply for a monitoring warrant, a Federal Court must first have been satisfied … that a control order should be issued. This requires the AFP to lead evidence to satisfy the court of a number of threshold issues outlined in Part 5.3 of the Criminal Code. This contrasts with a warrant issued for investigative

76 Attorney-General's Department, *Submission 9.1*, p. 18.

77 Australian Federal Police, *Submission 3*, p. 10.

78 Assistant Commissioner Neil Gaughan, Australian Federal Police, *Committee Hansard*, Canberra, 14 December 2015, p. 46.

79 Australian Federal Police, *Submission 3*, p. 10.

80 Attorney-General's Department, *Submission 9*, p. 7.

> purposes, where the information in the application has not been judicially considered.[81]

3.76 The Department further explained that including a 'reasonable suspicion' threshold, as suggested by several submitters, would not address the gap that the proposed monitoring power provisions are intended to fill. This is because

> [i]f there were reasonable grounds to suspect that the control order subject was contravening the terms of the control order or engaging in terrorism-related conduct, given both categories of conduct constitute criminal offences, law enforcement would be able to apply for warrants under the existing provisions for search, telecommunications interception or surveillance device powers for the purposes of investigating the commission of an offence.[82]

3.77 The Department also rejected the suggestion that the proposed monitoring powers regimes (including the TIA Act and SD Act provisions) would allow warrants to be issued 'automatically'. It noted that the fourth limb of the test as to whether the power sought is reasonably necessary or likely to substantially assist (in determining whether the control order has been, or is being, complied with)

> necessarily envisages that the issue of a monitoring warrant must consider the extent to which the grant of the warrants would assist in determining compliance. It will not necessarily be the case that such a warrant will assist, and will particularly depend on the conditions of a control order …
>
> Issuing authorities must also consider whether there is a possibility or risk that the person will engage in such conduct or breach the control order. The absence of any indications of a propensity or capacity to do so would for example weigh against the issuing of a warrant.[83]

3.78 Responding to concerns regarding the scope of monitoring powers and places at which monitoring powers could be exercised, the Department asserted that a monitoring search warrant

> can only be issued where it is reasonably necessary and reasonably appropriate and adapted to the prescribed purposes. This ensures

81 Attorney-General's Department, *Submission 9.1*, p. 19.

82 Attorney-General's Department, *Submission 9.1*, p. 19.

83 Attorney-General's Department, *Submission 9.1*, p. 22.

> that less intrusive means of gathering information will be used where possible.[84]

3.79 Moreover, the Department noted that even where a monitoring warrant is in force, 'any questioning or request for documents must be directed to one or more of the four prescribed purposes set out in paragraphs 3ZZKE(3)(c)-(f)'.[85]

3.80 While the Department agreed that the public interest must be balanced against the intrusion on the privacy of an individual, it rejected the contention that monitoring warrants should only be available where the relevant authority is satisfied that there are no less intrusive means of obtaining the information. The Department submitted:

> Introducing a requirement that a warrant only be issued where there is 'no less intrusive means' would, in effect, make the privacy intrusiveness of the power the primary consideration for issuing a warrant. This would subordinate other relevant considerations, such as the relative likely effectiveness of the different powers, operational imperatives or risks posed by the use of the different powers.
>
> For example, overt, physical surveillance may be less intrusive than an alternative power, but may also be likely to be significantly less effective than covert or electronic surveillance. The use of physical surveillance may also pose a greater risk to the safety of officers. Such an outcome would leave little scope for judgement on the part of the issuing authority in relation to whether, on balance, a monitoring warrant should be issued.[86]

3.81 The Department also drew a comparison with the privacy impact of ordinary search warrants, noting that

> current search warrant provisions have the effect that third parties may be affected by the execution of a search warrant … It is a matter for the issuing authority to determine, in the course of considering a search warrant application, whether it is appropriate for the warrant to authorise such searches.[87]

3.82 The Department further noted that:

84 Attorney-General's Department, *Submission 9.1*, p. 19.

85 Attorney-General's Department, *Submission 9.1*, p. 20.

86 Attorney-General's Department, *Submission 9.1*, p. 22.

87 Attorney-General's Department, *Submission 9.1*, p. 20.

- the power to issue a monitoring warrant is not delegable and can only be exercised by magistrates,[88]
- the Commonwealth Ombudsman has robust oversight powers to investigate complaints regarding the exercise of monitoring powers,[89] and
- there are existing rights of the person to seek remedies in relation to the unlawful exercise of police powers, as well as specific provision in the Bill for compensation for damage to electronic equipment.[90]

3.83 In relation to the role of the Queensland PIM, the Department stated that the Bill was modelled on the provisions of the standard search warrant regime in Part 1AA of the Crimes Act and the *Regulatory Powers (Standard Provisions) Act 2014*, which do not have a role for the PIM.[91] However, it also suggested that a State or Territory body like the PIM would not necessarily be excluded from the warrant application process under the SD Act provisions (discussed further below).[92]

Committee comment

3.84 The Committee notes concerns raised by submitters in relation to the impact of the proposed monitoring warrant regime on the privacy of a person subject to a control order as well as third parties.

3.85 The Committee also notes the potential constitutional implications of the proposed monitoring warrant regime for the validity of the control order regime, as identified by the Gilbert + Tobin Centre of Public Law.

3.86 It is vital that law enforcement has sufficient powers to be able to monitor a person's compliance with a control order consistent with the purposes for which a control order may be issued. Noting that the controls which may be placed on a person by a control order can include prohibitions or restrictions on their activities, whereabouts, associations and communications, the Committee does not consider it practicable to restrict the range of premises that may be subject to a monitoring warrant, or the means through which relevant evidence may be obtained.

3.87 The Committee notes the importance of ensuring that law enforcement has sufficient powers to detect breaches of control orders, as well as deter

88 Attorney-General's Department, *Submission 9.1*, p. 21.
89 Attorney-General's Department, *Submission 9.1*, p. 20.
90 Attorney-General's Department, *Submission 9.1*, p. 20.
91 Attorney-General's Department, *Submission 9.1*, p. 20.
92 Attorney-General's Department, *Submission 9.1*, p. 25.

individuals subject to control orders from attempting to breach their conditions. The Committee considers that a threshold of 'reasonable suspicion' for the monitoring warrant regime, as suggested by some submitters, would substantially reduce the utility of the proposed regime. However, the Committee notes the general comments made by the Independent National Security Legislation Monitor regarding the significance of these powers, and accordingly has recommended the inclusion of special advocates as a safeguard in Chapter 2 consistent with the Monitor's recommendations.

3.88 Given the extraordinary nature of these powers, the Committee considers it necessary to ensure that due regard is given to the intrusion on privacy and liberty when a monitoring warrant is issued. The Committee notes that Recommendation 37 of the COAG Review of Counter-Terrorism Legislation proposed a 'least interference' test in relation to the issuing of control orders. The Committee considers that there is value in applying a similar approach to the issuing of monitoring warrants for control orders. Accordingly, the Committee recommends that the issue of a monitoring warrant be subject to a requirement that the issuing officer have regard to whether the use of powers under the warrant constitutes the least interference with the liberty or privacy of any person that is necessary in all the circumstances.

3.89 As an additional safeguard, the Committee considers that persons required to answer questions or produce documents should be notified of their rights to claim privilege against self-incrimination and legal professional privilege.

3.90 The Committee notes concerns about the admissibility of evidence obtained in breach of the requirement not to execute a monitoring warrant if a control order is revoked, declared void, or varied by the removal of one or more controls, in civil proceedings. The Committee is satisfied that the rules of evidence, including the *Evidence Act 1995*, will apply, as with all criminal and civil proceedings, to ensure that such evidence will not be admitted unless a court considers the desirability of admitting the evidence outweighs the undesirability of admitting evidence improperly or illegally obtained.[93]

3.91 Use of the proposed regime should be subject to a level of oversight commensurate with the extraordinary nature of the powers granted. The

93 *Evidence Act 1995*, section 138. The factors that a court must take into account include the probative value of the evidence, the importance of the evidence in the proceedings, and the gravity of the impropriety or contravention of law and whether it was deliberate, reckless or inconsistent with a right of a person recognised by the International Covenant on Civil and Political Rights.

Commonwealth Ombudsman, as the Law Enforcement Ombudsman, possesses existing complaints-investigation powers and experience in relation to the AFP and responsibility for oversight of the telecommunications interception and surveillance devices regimes. The Committee considers that the Commonwealth Ombudsman is the appropriate body to provide oversight of the proposed regime and report to the Minister on the AFP's compliance with the requirements of the regime. The Commonwealth Ombudsman's oversight would be enabled by a requirement for all records relating to monitoring warrants to be kept, consistent with existing requirements under the current *Telecommunications (Interception and Access) Act 1979* (TIA) and *Surveillance Device Act 2004* (SD Acts). This requirement should also be accompanied by a requirement for the AFP to report to the Commonwealth Ombudsman any breaches detected in relation to the legislative requirements.

3.92 Further, the Committee accepts that the extraordinary nature of the proposed monitoring powers demands ongoing review by the Parliament as to the necessity of such powers and their use over time. Accordingly, the Committee recommends that the Bill provide for annual reporting to the Parliament, consistent with the control order reporting requirements in section 104.29 of the Criminal Code. The Committee notes that the TIA and SD Acts contain comprehensive annual reporting requirements, and considers that these requirements should also apply to the amendments in Schedules 9 and 10 of the Bill.

Recommendation 9

The Committee recommends that for a monitoring warrant in relation to a premises or person, the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 be amended to reflect the intent of Recommendation 37 of the Council of Australian Governments Review of Counter-Terrorism Legislation, to explicitly require that:

- **the issuing officer is to have regard to whether the exercise of monitoring powers under the warrant constitutes the least interference with the liberty or privacy of any person that is necessary in all the circumstances.**

Recommendation 10

The Committee recommends that the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 be amended to require the Australian Federal Police to notify persons required to answer questions or produce documents by virtue of a monitoring warrant of their right to claim privilege against self-incrimination and legal professional privilege.

Recommendation 11

The Committee recommends that the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 be amended to require the Australian Federal Police (AFP) to notify the Commonwealth Ombudsman within six months following the exercise of monitoring powers. This requirement should also apply to telecommunications interception (TI) and surveillance device (SD) control order warrants under Schedules 9 and 10.

The Committee further recommends that the Bill be amended to require:

- **the AFP to retain all relevant records in relation to the use of monitoring warrants or the exercise of monitoring powers, including for TI and SD control order warrants under Schedules 9 and 10, consistent with existing requirements in relation to other TI and SD warrants,**
- **the AFP to notify the Commonwealth Ombudsman as soon as practicable of any breaches of the monitoring powers requirements, including for TI and SD warrants under Schedules 9 and 10, and**
- **the Commonwealth Ombudsman to report to the Attorney-General annually regarding the AFP's compliance with the requirements of the monitoring powers regime, including for TI and SD warrants under Schedules 9 and 10, and deferred reporting for those warrants.**

Recommendation 12

The Committee recommends that the Attorney-General be required to report annually to the Parliament on the Australian Federal Police (AFP) use of the monitoring powers regime as part of the control order reporting requirements set out in section 104.29 of the Criminal Code. The matters to be included in the report, mirroring the relevant requirements in section 104.29, are:

- **the number of monitoring warrants issued,**
- **the number of instances on which powers incidental to the issue of a monitoring warrant were exercised,**
- **particulars of:**
  - ⇒ **any breaches self-reported to the Commonwealth Ombudsman**
  - ⇒ **any complaints made or referred to the Commonwealth Ombudsman relating to the exercise of monitoring powers, and**
- **any information given under section 40SA of the *Australian Federal Police Act 1979* that related to the exercise of monitoring powers and raised an AFP conduct or practices issue (within the meaning of that Act).**

The Committee also recommends that the Attorney-General ensure that the telecommunications interception and surveillance device control order warrants provided for in Schedules 9 and 10 of the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 are comprehensively covered by the annual reporting requirements in the *Telecommunications (Interception and Access) Act 1979* and *Surveillance Devices Act 2004.*

3.93 The Committee's functions were expanded in 2014 to include reporting to the Parliament on any matter 'appertaining to the AFP or connected with the performance of its functions under Part 5.3 of the *Criminal Code*'.[94] The Committee first reported on the AFP's functions in its 2014–2015 Annual Report.[95] The Committee intends that future annual reports will be informed by the Attorney-General's report to the Parliament on the control order regime.

94 *Intelligence Services Act 2001*, paragraph 29(1)(bab).

95 Parliamentary Joint Committee on Intelligence and Security, *Annual Report of Committee Activities 2014–2015*, September 2015, pp. 12–14, 25–27.

Telecommunications interception (Schedule 9)

3.94 Under Schedule 9 of the Bill the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) would be amended to allow agencies to apply to a judge or nominated member of the Administrative Appeals Tribunal (the AAT) for a TI warrant for the control order monitoring purposes (a TI control order warrant).

3.95 Under sections 46 and 46A of the TIA Act, warrants may be issued with respect to a telecommunications service, or with respect to a person (termed 'telecommunications service warrants' and 'named person warrants', respectively). Whereas a telecommunications service warrant authorises interception of a particular telecommunications service,[96] a named person warrant authorises the interception of communications made to or from any telecommunications service that a particular person is using or is likely to use, or the interception of communications made by means of one or more particular telecommunications devices that the person is using or is likely to use.[97]

3.96 Telecommunications service warrants and named person warrants authorise the interception of communications made to or from a telecommunications service where information that would likely be obtained would likely assist in connection with the investigation of a serious offence, or serious offences, in which the particular person is involved.[98]

3.97 Under section 46, warrants may also authorise the interception of communications made to or from the telecommunications service to assist in connection with the investigation of a serious offence, or serious offences, in which *another* person is involved, with whom the particular person is likely to communicate using the service (so-called 'B-party warrants').[99]

3.98 The proposed amendments would allow warrants to be issued under these provisions where there is a control order in force in relation to a person (where a serious offence or serious offences are not being investigated). Section 46 would be amended by the insertion of proposed subsections 46(4)–(6), which would allow a telecommunications service warrant to be issued where:

96 *Telecommunications (Interception and Access) Act 1979*, subsection 46(1).

97 *Telecommunications (Interception and Access) Act 1979*, subparagraphs 46A(1)(d)(i)–(ii).

98 *Telecommunications (Interception and Access) Act 1979*, subparagraph 46(1)(d)(i), paragraph 46A(1)(d).

99 *Telecommunications (Interception and Access) Act 1979*, subparagraph 46(1)(d)(ii).

- there are reasonable grounds to suspect a particular person is using or is likely to use, the telecommunications service, and
- a control order is in force in relation to the person using the service, or
- a control order is in force in relation to another person and the person using the service is likely to communicate with the subject of the control order using the service (a 'B-party warrant'), and
- information that would likely be obtained under the warrant would be likely to substantially assist in connection with the control order monitoring purposes.

3.99 Section 46A would be amended by the insertion of proposed subsections 46A(2A) and (2B), which would allow a named person warrant to be issued where:

- there are reasonable grounds for suspecting that a person is using or is likely to use more than one telecommunications service,
- a control order is in force in relation to a person, and
- information that would likely be obtained by intercepting:
  - ⇒ communications made to or from any telecommunications service the person is using or is likely to use, or
  - ⇒ communications made by means of a particular telecommunications device or particular telecommunications devices that the person the person is using or is likely to use,

  would likely substantially assist in connection with the control order monitoring purposes.

3.100 Prior to issuing either a telecommunications service or named person warrant for control order monitoring purposes, the judge or AAT member must have regard to certain matters. These matters include:

- how much the privacy of any person or persons would likely be interfered with,
- how much information likely to be obtained under the warrant would be likely to assist with the control order monitoring purposes,
- to what extent other methods for those purposes that do not involve the interception are available, and

- the possibility that the subject of the control order has engaged or will engage in conduct connected to the control order monitoring purposes.[100]

3.101 The issuing of B-party warrants for control order monitoring purposes would additionally be restricted by the requirement that, prior to issuing such a warrant, the judge or AAT member must also be satisfied that the agency has exhausted all other practicable methods of identifying the telecommunications service used or likely to be used by the subject of the control order, or that that interception of communications made to or from a telecommunications service used or likely to be used by the subject of the control order would not otherwise be possible.[101]

3.102 An application for a TI warrant would be able to made, and the warrant issued, prior to the control order being served on the person.[102] The Explanatory Memorandum provides the following rationale:

> Warrant applications and the subsequent process of provisioning an interception warrant can take a considerable period of time. If agencies were required to wait for a control order to be in force to apply for a warrant critical time may be lost to the time taken to then obtain and provision the warrant.[103]

3.103 The revocation provisions under the TIA Act would apply to control order warrants.[104] In particular, the requirement for the chief officer of an agency to revoke a warrant if satisfied that the grounds on which the warrant was issued have ceased to exist will extend to circumstances where the control order, or any succeeding control order, are no longer in force.[105] Further, under section 58 of the TIA Act, the chief officer must immediately take such steps as are necessary to discontinue the interception of communications on the revocation or proposed revocation of a warrant.

3.104 Records of the particulars of TI warrants issued for control order monitoring purposes would need to be kept under the proposed provisions.[106]

3.105 The current provisions in relation to public reporting of TI warrants would be amended to provide for the deferral of reporting in relation to TI control order warrants. This would occur where the information contained

100 See proposed subsections 46(5) and 46A(2B).

101 Proposed subsection 46(6).

102 Proposed section 6T.

103 Explanatory Memorandum, pp. 84–85.

104 See *Telecommunications (Interception and Access) Act 1979*, section 57.

105 Item 28 of the Bill.

106 Items 38–43 of the Bill.

in the public report would be capable of revealing whether or not a TI control order warrant is in force in relation to a telecommunications service being used by, or in relation to, a particular person.[107]

Use of information

3.106 The proposed provisions would also amend the definition of 'permitted purpose' under existing subsection 5(1) of the TIA Act to allow the communication, use and recording by State and Territory police of lawfully intercepted information (that is, information intercepted under a TI warrant)[108] and interception warrant information (information about an application for, issue of, existence or non-existence of, or the expiry of a TI warrant, or any other information likely to enable the identification of a telecommunications service or person to which a TI warrant relates)[109] for purposes connected with the Commonwealth control order regime and with the State and Territory PDO regimes.[110]

3.107 The definition of 'exempt proceeding' in subsection 5B(1) of the TIA Act would be amended to allow lawfully intercepted information and interception warrant information to be given in proceedings relating to the State and Territory PDO regimes.[111] Such information can already be given in evidence in proceedings related to control orders and Commonwealth PDOs.[112]

3.108 Lawfully accessed information (which is information obtained by accessing stored communications, such as text messages or email, under warrant) would also be able to be communicated, used and recorded by police for purposes connected with control orders and the PDO regimes nationally.[113]

3.109 The Bill would allow for the limited retention and use of information obtained under a TI control order warrant where the interim control order which provided the basis for the warrant is subsequently declared void by a court.

107 Proposed section 103B.

108 *Telecommunications (Interception and Access) Act 1979*, section 6E.

109 *Telecommunications (Interception and Access) Act 1979*, section 6EA.

110 Item 3 of the Bill. See also section 67 of the *Telecommunications (Interception and Access) Act 1979*, which relates to dealings for a permitted purpose.

111 Item 7 of the Bill. See also section 74 of the *Telecommunications (Interception and Access) Act 1979*.

112 See paragraphs 5B(1)(bb) and 5B(1)(bc), and section 74 of the *Telecommunications (Interception and Access) Act 1979*.

113 Proposed section 139B. See also the definitions of 'lawfully accessed information' and 'stored communication' in subsection 5(1) of the *Telecommunications (Interception and Access) Act 1979*.

3.110 Section 79 of the TIA Act provides that the chief officer of an agency must cause a restricted record in the possession of the agency to be destroyed if the chief officer is satisfied that the record is not likely to be required for a permitted purpose in relation to the agency.[114] The Bill proposes to insert a section 79AA, which provides that the chief officer must cause information obtained under a TI control order warrant issued prior to the control order being served on the person to be destroyed if the warrant was issued for the purpose of determining compliance with the control order. This requirement would apply unless the chief officer is satisfied that the information is likely to assist in the protection of the public from a terrorist act, or preventing the provision of support for, or the facilitation of, a terrorist act or hostile activity in a foreign country.[115]

3.111 Under proposed section 299, information obtained under a TI control order warrant where the interim control order is subsequently declared by a court to be void would only be able to be communicated, used, recorded or given in evidence in a proceeding in limited circumstances. This would be where the person reasonably believes that doing so is necessary to assist in preventing, or reducing the risk of, the commission of a terrorist act, serious harm to a person or serious damage to property, or for purposes connected with Commonwealth, State or Territory PDO laws.[116]

Matters raised in evidence

3.112 As with the proposed monitoring warrant regime, submitters expressed concern regarding the threshold for issuing a TI control order warrant and the impact on the privacy of both the individual subject to the control order and third parties.[117]

3.113 The proposed subsection 46(5) mirrors existing requirements in the TIA Act for an issuing judge or AAT member to have regard to how much the privacy of any person or persons would be likely to be interfered with. However, some submitters did not consider this was adequate. The Australian Human Rights Commission submitted:

> While there are requirements that issuing authorities take a number of other factors into account, including the extent to which any person's privacy would be affected and whether there are

114 'Restricted record' is defined in subsection 5(1) of the *Telecommunications (Interception and Access) Act 1979* as 'a record other than a copy, that was obtained by means of an interception … of a communication passing over a telecommunications system'.

115 Proposed paragraph 79AA(1)(e).

116 Proposed paragraphs 299(2)(e)–(f), and proposed subsection 299(3).

117 Australian Human Rights Commission, *Submission* 5, p. 18; Law Council of Australia, *Submission 6*, p. 17; Joint councils for civil liberties, *Submission 17*, p. 15.

> alternative means of obtaining the information, the Commission considers these requirements are insufficient in [the] circumstances.[118]

3.114 The Commission went on to state that:

> It is necessary to bear in mind that control orders are granted following a civil hearing, determined on the civil standard of proof. The subject of the order need not have been charged with or convicted of any offence. In those circumstances, the Commission considers that it has not been demonstrated that it would be appropriate to allow for the highly intrusive monitoring or surveillance which would be authorised by these amendments …[119]

3.115 Accordingly, the Commission recommended that the threshold for the issue of a TI control order warrant be raised and that its suggested 'no less intrusive means' requirement also apply in the same terms as for the proposed monitoring warrants.[120]

3.116 Similarly, the Muslim Legal Network (NSW) submitted that the balancing of privacy concerns and the extent to which interception would assist in preventing terrorist and related acts or monitoring compliance with a control order was not sufficient to address the privacy implications of the proposed amendments.[121]

3.117 Such concerns appeared to be closely related to the proposed inclusion of 'B-party warrants' for the monitoring of compliance with a control order. The Law Council of Australia described B-party warrants as 'particularly invasive tools for detection of criminal activity',[122] while the joint civil liberties councils submitted that B-party warrants 'are a serious and unjustifiable invasion of a non-suspect person's right to privacy.'[123] Both of these submitters argued that the proposed regime lowers the threshold for which a B-party warrant may be issued from investigation of a serious offence punishable by seven years' imprisonment to a control order breach punishable by five years' imprisonment.[124]

118 Australian Human Rights Commission, *Submission 5*, pp. 17–18.

119 Australian Human Rights Commission, *Submission 5*, p. 18.

120 Australian Human Rights Commission, *Submission 5*, p. 18.

121 Muslim Legal Network (NSW), *Submission 11*, p. 29.

122 Law Council of Australia, *Submission 6*, p. 18.

123 Joint councils for civil liberties, *Submission 17*, p. 16.

124 Joint councils for civil liberties, *Submission 17*, p. 16. See also Law Council of Australia, *Submission 6*, p. 18.

3.118 Concerns were also raised about the use of a TI control order warrant prior to a control order being served on a person. Australian Lawyers for Human Rights stated:

> We do not agree that new section 6T, which treats a control order as effective even if has not been able to be served on the person in question, is appropriate. This provision enables monitoring of a person on the basis of a control order, before they are even aware that they are the subject of a control order. According to [the Explanatory Memorandum, paragraph 158], referring to the *Surveillance Devices Act*, this appears to be **intended 'to ensure that officers have an opportunity to install surveillance devices covertly**, as there are often limited opportunities to do so'.[125]

3.119 Other privacy issues raised by submitters related to the use of information obtained under the proposed amendments. The Law Council of Australia noted that proposed section 139B will enable lawfully accessed information to be communicated for a broad range of purposes in the context of control orders and PDOs, and recommended further scrutiny of this provision by the Privacy Commissioner.[126]

3.120 The Council also noted the absence of a specific provision in Schedule 9 similar to proposed section 3ZZOD in Schedule 8, imposing a requirement not to execute a TI control order warrant if the control order is revoked, declared void or varied by removing one or more obligations, prohibitions or restrictions.[127] However, the Bill amends section 57 of the TIA Act to require a TI control order warrant to be revoked if the control order or any succeeding control order has ceased to be in force.[128]

3.121 The Muslim Legal Network (NSW) submitted that there should be a complete prohibition on the use of information obtained under a TI control order warrant issued under the proposed amendments if the control order is subsequently declared void.[129]

3.122 The Network also did not support giving the chief officer of the interception agency the ability to determine whether information obtained under a TI control order warrant, issued for the purpose of determining compliance with a control order, prior to the control order being served, should be destroyed. It contended that

125 Australian Lawyers for Human Rights, *Submission 4*, p. 5. Emphasis in the original.

126 Law Council of Australia, *Submission 6*, p. 20.

127 Law Council of Australia, *Submission 6*, p. 20.

128 Item 28 of the Bill.

129 Muslim Legal Network (NSW), *Submission 11*, p. 30.

> leaving this determination at the discretion of the chief officer is problematic, particularly where the chief officer may have a vested interest in showing that the information obtained under such a warrant assists in the prevention or facilitation of a terrorist act …
>
> Furthermore, it would seem that the decision to be made by the chief officer is only examined by the ombudsman under the amendments to sections 83 and 85 of the Act.[130]

3.123 Accordingly, the Network called for oversight of such decisions by a judge or AAT member, arguing that would be consistent with the issuing of the warrants.[131]

3.124 The deferred reporting provisions attracted some comments by submitters in the context of the TIA Act provisions. They will be discussed in the next section as such comments also apply to the SD Act provisions.

3.125 The comments of the AFP and Attorney-General's Department in relation to the operational imperative to effectively monitor compliance with control orders, referred to above, are also relevant to the proposed amendments to the TIA Act.[132] The AFP's submission noted

> Search, telecommunications interception and surveillance powers are particularly relevant to monitoring a person's compliance with obligations, prohibitions and restrictions in relation to:
>
> - the possession of specified articles or substances;
> - communication or association with specified individuals;
> - access or use of specified telecommunications or technology, including the internet; and
> - the carrying out of specified activities.[133]

3.126 The Attorney-General's Department explained in its submission the rationale for provisions relating to the use of lawfully intercepted information in PDO proceedings. It submitted:

> At the Commonwealth level, and in approximately half of all States and Territories, applications for preventative detention orders are by way of an application to an 'issuing authority'. However, in the remaining States and Territories, applications are made by way of proceedings before a court. Accordingly, in these States and Territories, there is a risk that a court would determine that lawfully intercepted information may not be given in

130 Muslim Legal Network (NSW), *Submission 11*, p. 31.

131 Muslim Legal Network (NSW), *Submission 11*, pp. 30–31.

132 See paragraphs 3.69–3.73 above.

133 Australian Federal Police, *Submission 3*, p. 10.

> evidence in a proceeding for the application for a preventative detention order …
>
> In the Department's view, this represents an anomaly in the legislation. Whether the application for a preventative detention order is made by an issuing authority acting in his or her personal capacity, or whether it is made by a court, should not affect the ability for telecommunications interception and surveillance device information to be relied upon as part of the application.[134]

3.127 Responding to concerns about the availability of B-party warrants for monitoring compliance with a control order, the Department explained that

> B-party warrants assist interception agencies to counter measures adopted by persons of interest to evade telecommunications interception, such as adopting and discarding multiple telecommunications services. The ability, as a last resort, to intercept the communications of an associate of a person of interest will ensure that the utility of interception is not undermined by evasive techniques adopted by those subject to a monitoring warrant.[135]

3.128 It also outlined the additional requirements that apply to B-party warrants compared to other interception warrants.[136]

3.129 The Department noted that information obtained under a control order that is subsequently declared void can only be admitted into proceedings related to preventing or reducing the risk of the commission of a terrorist act, serious harm to a person or serious damage to a property, or a Commonwealth, State or Territory PDO.[137] Section 63 of the TIA Act and section 45 of the SD Act prohibit dealing in information obtained for any purpose unless an express exception applies, overriding the provisions of the *Evidence Act 1995* and other common law discretions which allow evidence to be admitted where the public interest outweighs the undesirability of admitting it, in light of the manner in which the evidence was obtained.

3.130 Accordingly, the Bill provides for limited exceptions to use and adduce such information in proceedings, but does not affect the court's discretion

134 Attorney-General's Department, *Submission 9*, pp. 9–10.

135 Attorney-General's Department, *Submission 9.1*, p. 23.

136 Attorney-General's Department, *Submission 9.1*, pp. 23–24.

137 Attorney-General's Department, *Submission 9.1*, p. 24.

to refuse to admit evidence, or its duty to refuse to admit improperly obtained evidence in particular circumstances.[138]

Committee comment

3.131 The Committee acknowledges concerns raised by submitters in relation to the potentially significant privacy impacts of TI control order warrants on third parties in particular.

3.132 However, while the seriousness of a breach of a control order may vary depending on the circumstances, the purposes for which a control order is issued are invariably serious. Therefore, the ability to monitor compliance with a control order is important in deterring breaches that may have grave consequences for community safety.

3.133 The Committee considers that the proposed safeguards surrounding the issuing of TI control order warrants within the Bill are appropriate and proportionate in light of the objectives and rationale for the legislation. It is noted that, of the range of 'serious offences' in relation to which a TI warrant is currently available, although many are punishable by seven–year prison terms, the length of the prison term is not a determinative factor for inclusion in that list.

3.134 The power to intercept communications is vital to ensuring compliance with certain conditions that may be imposed under a control order, such as restrictions or prohibitions on communicating or associating with specified individuals, accessing or using specified telecommunications or technology, and carrying out specified activities, can be effectively monitored. Such a power must be covert, in order to obtain information that can be used to accurately assess a person's intentions or behaviour. The deferred reporting provisions in the Bill are appropriate to balance the protection of the covert nature of the power and the need for accountability and transparency.

3.135 The Committee believes that robust accountability and oversight of the proposed provisions is the key to ensuring the protection of individual rights, and guarding against unjustified intrusions into privacy or abuse of police powers. The Committee is satisfied that the oversight of the Commonwealth Ombudsman, which is responsible for overseeing the existing TIA and SD Act regimes, will ensure there is appropriate accountability for the use of the proposed provisions. The Committee considers that a requirement for the AFP to proactively report any

138 Attorney-General's Department, *Submission 9.1*, p. 24.

breaches of the legislative requirements to the Ombudsman would further strengthen this accountability (see recommendation under Schedule 8).

3.136 As with the monitoring powers regime, the Committee considers that the overall effectiveness and justification for the TI control order warrants regime should be subject to ongoing review by Parliament. The Committee considers that, subject to the deferred reporting arrangements, TI control order warrants should also be covered by the existing annual reporting requirements contained in the TIA Act.

3.137 The Committee has earlier recommended a 'least interference' test to require that due regard is given to the intrusion on privacy and liberty when a monitoring warrant is issued under Schedule 8 of the Bill. The Committee notes that Schedule 9 of the Bill already contains provisions requiring the judge or AAT member to have regard to the likelihood that the privacy of any person would be interfered with, the likely usefulness of any information that would be obtained, and the extent to which other methods that do not involve interception are available, in determining whether a TI control order warrant should be issued. The Committee considers these provisions should be strengthened to include a more explicit 'least interference' test.

Recommendation 13

The Committee recommends that for a telecommunications interception control order warrant, the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 be amended to reflect the intent of Recommendation 37 of the Council of Australian Governments Review of Counter-Terrorism Legislation, to explicitly require that:

- **the issuing officer is to have regard to whether the interception of telecommunications under the warrant constitutes the least interference with the liberty or privacy of any person that is necessary in all the circumstances.**

Surveillance devices (Schedule 10)

3.138 Schedule 9 of the Bill would amend the *Surveillance Devices Act 2004* (SD Act) to allow law enforcement officers to obtain warrants for the installation and use of surveillance devices (SDs) and to obtain tracking device authorisations for control order monitoring purposes.

3.139 Under the amendments, law enforcement officers would be able to apply to a judge or nominated AAT member for the issue of a control order warrant to use an SD (an SD control order warrant). In order to make the application, there must be a control order in force and the officer must suspect on reasonable grounds that the use of an SD to obtain information relating to the subject of the control order would be likely to substantially assist in the control order monitoring purposes.[139] An application would be able to be made and the warrant issued prior to the control order having been served on the person.[140]

3.140 Prior to issuing an SD control order warrant, the issuing officer must be satisfied that a control order is in force and that use of the SD would be likely to substantially assist in the control order monitoring purposes.[141] The issuing officer must have regard to the likely value of the information sought to be obtained to the control order monitoring purposes, the possibility that the subject of the control order has or will engage in conduct connected to the control order monitoring purposes, and also any previous SD control order warrants sought in relation to that person.[142]

3.141 The revocation provisions under the SD Act would apply to control order warrants.[143] A judge or nominated AAT member may revoke a warrant prior to its expiry on their own initiative,[144] or in certain circumstances, the chief officer of the relevant law enforcement agency must revoke a warrant. These circumstances would include where the warrant is no longer required for the control order monitoring provisions or if no control order is in force.[145] In addition to revoking the control order

139 See proposed subsection 14(3C).

140 See proposed section 6C.

141 See proposed paragraph 16(1)(bc).

142 See proposed paragraphs 16(2)(eb), 16(2)(ec) and 16(2)(g).

143 See section 20.

144 Subsection 20(1).

145 Item 17 of the Bill.

warrant, the chief officer would also be required to take steps to discontinue the use of the warrant as soon as practicable.[146]

3.142 Existing provisions in the SD Act allow the limited use of optical SDs without a warrant, in circumstances where this will not involve entry onto premises without permission or interference without permission with any vehicle or thing.[147] The existing provisions already allow Commonwealth law enforcement officers to do this in the course of their duties within the functions of the AFP, but State and Territory law enforcement officers may only do so in the investigation of a relevant offence.[148] The proposed provisions would amend section 37 so that State and Territory law enforcement officers acting in the course of their duties may use optical SDs without a warrant to obtain information about the activities of the subject of a control order for the control order monitoring purposes.[149]

3.143 SDs may also currently be used without a warrant for the purpose of listening to or recording words spoken in limited circumstances.[150] The amendments would extend these provisions to State or Territory law enforcement officers or persons assisting State or Territory law enforcement officers for control order monitoring purposes.[151]

3.144 In addition, as noted above, the Bill would amend the existing tracking device provisions to permit law enforcement officers to use tracking devices for obtaining information about the subject of a control order for the control order monitoring purposes.[152] This must be with the written permission of an appropriate authorising officer, which must not be given for the use, installation or retrieval of the tracking device if that would involve entry onto premises without permission or interference without permission with any vehicle or thing.[153]

3.145 Details of the particulars of SD warrants issued for the control order monitoring purposes would need to be reported to the Minister for Justice under existing reporting provisions.[154] In addition, proposed subsection 49(2A) would require information about the benefit of the use of an SD for the control order monitoring purposes and details of the general use of

146 See proposed subsections 21(3C) and 21(3D).

147 See section 37.

148 Subsection 37(2).

149 See proposed subsection 37(4).

150 Section 38.

151 See proposed subsections 38(3A) and 38(6).

152 See proposed subsection 39(3B).

153 See subsection 39(8).

154 See proposed subparagraph 49(2)(b)(xb).

information or evidence obtained by the use of the SD. The Explanatory Memorandum states:

> This will ensure that law enforcement agencies are required to document and report the value of the use of surveillance devices used in relation to a control order.[155]

3.146 Current provisions in relation to public reporting of SD warrants would be amended to require in limited circumstances that reporting of SD control order warrants be deferred until a subsequent report. These circumstances relate to where the information contained in the public report would be capable of revealing whether a SD control order warrant is likely to be, or not likely to be, in force in relation to particular premises, a particular object or class of object, or the conversations, activities or location of a particular person.[156]

Use of information

3.147 Under existing section 45 of the SD Act, the unlawful use, recording, communication or publication of 'protected information' is prohibited, subject to limited exceptions.[157] Similarly, protected information may not be admitted in evidence in any proceedings, subject to limited exceptions.[158]

3.148 Schedule 10 would amend the existing provisions relating to the use of protected information in several ways. The amendments would allow protected information to be used in control order proceedings and PDO proceedings nationally, by adding these proceedings to the definition of 'relevant proceedings' under existing subsection 6(1) and by amending the definition of 'State and Territory relevant proceeding' under subsection 45(9).[159]

3.149 Further, information:

- obtained under a SD control order warrant,
- likely to enable the identification of a person, object or premises specified in a control order warrant,

155 Explanatory Memorandum, page 104.

156 See proposed section 50A.

157 'Protected information' is defined in section 44 of the *Surveillance Devices Act 2004*, and includes information obtained from the use of a surveillance device under warrant or tracking device authorisation.

158 Subsections 45(3)–(5).

159 See items 5 and 31.

- obtained under a tracking device authorisation issued for control order monitoring purposes, or
- likely to enable the identification of a person, object or premises specified in a tracking device authorisation

would be able to be used, recorded, communicated, published or admitted into evidence to determine whether a control order is being complied with.[160]

3.150 Proposed section 65B would permit the use of information obtained under a SD control order warrant where the interim control order which provided the basis for the warrant is subsequently declared void by a court. This provision would relate to information obtained using:

- a surveillance device authorised by a control order warrant issued under section 14 on the basis that an interim control order was in force,
- an optical surveillance device authorised (without warrant) under section 37 on the basis that an interim control order was in force and used for control order monitoring purposes,
- a surveillance device authorised (without warrant) under section 38 on the basis that an interim control order was in force and used for control order monitoring purposes, or
- a tracking device authorised (without warrant) under section 39 on the basis that an interim control order was in force and used for control order monitoring purposes

as long as the information was obtained while the interim control order was in force.

3.151 The information would be able to be given in evidence, used, recorded or communicated by a person if the person reasonably believes that doing so is necessary to assist in preventing, or reducing the risk of, the commission of a terrorist act, serious harm to a person or serious damage to property, or for purposes connected with PDOs under Commonwealth, State or Territory laws.[161]

3.152 Proposed section 46A would require the destruction as soon as reasonably practicable of information obtained under a SD control order warrant or control order tracking device authorisation for the purpose of determining compliance with a control order, where the information was obtained prior to the control order being served. This requirement would not apply

160 See proposed paragraphs 45(5)(j) and 45(5)(k).

161 See proposed subsections 65B(2) and 65B(3).

where the information would be likely to assist in protecting the public from a terrorist act, or preventing the provision of support for or facilitation of a terrorist act or hostile activity in a foreign country. The Explanatory Memorandum states that this provision

> reflects the overwhelming public interest in law enforcement agencies being permitted to use information in their possession to prevent acts of terrorism and hostile activity in foreign countries.[162]

Matters raised in evidence

3.153 As with Schedules 8 and 9 relating to monitoring warrants and TI control order warrants, there were several submissions regarding the privacy and human rights impacts of the SD Act amendments.[163] The joint civil liberties councils submitted that they

> have the same general unease in relation to these proposals as [they] do to the monitoring and surveillance proposals in schedules 8 and 9.[164]

3.154 The Law Council of Australia submitted that the threshold for a SD control order warrant under Schedule 10 should require, at a minimum, a reasonable suspicion that the control order is not being complied with or that the individual is engaged in terrorist-related activity. The Council recommended this with respect to the proposed monitoring warrants and TI control order warrants.[165]

3.155 Similarly, the Australian Human Rights Commission applied its recommendations in relation to the threshold and availability of monitoring warrants and TI control order warrants to the proposed surveillance devices regime.[166]

3.156 The Law Council of Australia also raised concerns regarding proposed subsection 38(6), which allows a 'person assisting' a State or Territory law enforcement officer to use a surveillance device without warrant in relation to determining whether a control order has been, or is being, complied with. The Council suggested that this provision would extend to informants, and submitted that

162 Explanatory Memorandum, page 103.

163 Australian Lawyers for Human Rights, *Submission 4*, p. 4; Australian Human Rights Commission, *Submission 5*, pp. 16–18; Law Council of Australia, *Submission 6*, pp. 16–17, 20–23; Muslim Legal Network (NSW), *Submission 11*, pp. 32–34; Joint councils for civil liberties, *Submission 17*, p. 17.

164 Joint councils for civil liberties, *Submission 17*, p. 17.

165 Law Council of Australia, *Submission 6*, p. 17.

166 Australian Human Rights Commission, *Submission 5*, p.18.

> [if] evidence is obtained from informants without judicial oversight, then such evidence comes at too high a price … If such investigative steps are to be used, they should only be taken following the lawful approval of a warrant.[167]

3.157 The Council further suggested that the Committee should seek the view of the Privacy Commissioner in relation to the extension of the range of 'relevant proceedings' for which information obtained through the use of a surveillance device warrant can be used.[168] These amendments relate to the use of such information in control order proceedings under Division 104 of the Criminal Code and PDO proceedings under relevant Commonwealth, State and Territory legislation.[169]

3.158 The Muslim Legal Network (NSW) raised concerns regarding the use of information obtained under the proposed surveillance device provisions in relation to an interim control order which is subsequently declared void by a court. It considered that proposed section 65B would allow the storage and use of such information which, it submitted, 'stands in contrast with, and seeks to undermine, the utility of the safeguard put in place by section 46A'.[170]

3.159 Specifically, the Network expressed concern that proposed subsection 65B(3) would allow such information to be used as evidence in proceedings related to 'serious offences'.[171] It submitted that this would increase the risk of abuse of such powers by law enforcement agencies,[172] and 'reduce the role of courts to decide upon the propriety and allowance of evidence in proceedings'.[173] In particular, it highlighted the fact that senior members of the AFP have the power to make initial PDOs, and submitted that proposed subsection 65(4) would allow the AFP to more easily make such orders.[174]

3.160 The Network also expressed concerns that the proposed deferred reporting provisions would undermine transparency and accountability in relation to the control order regime. It submitted:

> Providing an avenue for the Executive to escape disclosure of important information regarding criminal sanctions laid on

167 Law Council of Australia, *Submission 6*, p. 21.

168 Law Council of Australia, *Submission 6*, p. 20.

169 Proposed paragraphs 6(1)(q)–(z).

170 Muslim Legal Network (NSW), *Submission 11*, p. 33.

171 Muslim Legal Network (NSW), *Submission 11*, p. 33.

172 Muslim Legal Network (NSW), *Submission 11*, pp. 33–34.

173 Muslim Legal Network (NSW), *Submission 11*, p. 34.

174 Muslim Legal Network (NSW), *Submission 11*, p. 34.

> individuals is deeply concerning as it damages transparency. Lack of information in Parliament means that periodic review of this newly introduced legislative scheme (ie the surveillance of control order subjects) by members of Parliament will not take place.
>
> It also means that members of the public and media will be unable to access, or report on, this information. This will damage the freedom with which the decision-making process, performance and impartiality of law enforcement agencies can be assessed.[175]

3.161 Australian Lawyers for Human Rights submitted that the rationale for deferred reporting proffered by the Explanatory Memorandum was 'not convincing', arguing that

> it is quite clear from the legislation and the [Explanatory Memorandum] that any person who is the subject of a control order will be subject to intensive electronic and other surveillance …[176]

3.162 The joint submission from a range of media organisations commented that the deferred reporting provisions represented a choice to prioritise security considerations over the public interest in the free flow of information, and submitted that

> [t]he public discourse surrounding national security laws which impinge on the freedom of the media needs to acknowledge this compromise, rather than suggesting a balance has been achieved.[177]

3.163 The joint media organisations recommended oversight of the deferred reporting provisions by the Commonwealth Ombudsman and/or the Inspector-General of Intelligence and Security. They submitted that this would

> ensure that information is made publicly available within the most appropriate timeframes, and there are checks and balances in place to ensure the Australian public's right to know is met – without jeopardising national security and the safety of the public and our law enforcement and security personnel.[178]

3.164 The Law Council of Australia acknowledged the importance of reporting obligations not jeopardising ongoing investigations. However, it submitted that proposed section 50A of the SD Act as drafted would mean

175 Muslim Legal Network (NSW), *Submission 11*, pp. 32–33.

176 Australian Lawyers for Human Rights, *Submission 4*, p. 5.

177 Joint media organisations, *Submission 10*, p. 2.

178 Joint media organisations, *Submission 10*, p. 2.

that it was unlikely that reporting would occur where a surveillance device warrant had been but was no longer in force.[179] Accordingly, the Council suggested that these provisions be redrafted or that the phrase 'or is not likely to be' removed.[180]

3.165 As with Schedule 8, the Queensland Government submitted that in relation to an application for a surveillance device warrant by a Queensland interception agency, issuing authorities should be required to have regard to any submissions made by the Queensland PIM.[181]

3.166 Noting the requirement that the Queensland PIM report annually with respect to control orders, the Queensland Government also recommended that the provisions be amended to provide for deferred public reporting by the Queensland PIM on the use of surveillance device warrants.[182]

3.167 The Attorney-General's Department explained that the issues necessitating the provisions relating to the use of information obtained by surveillance device in PDO proceedings were similar to those arising under the telecommunications interception regime, discussed at paragraph 3.124 above.[183]

3.168 In its supplementary submission, the Attorney-General's Department responded to concerns regarding the use of surveillance devices without warrant, explaining that the Bill

> makes the full range of surveillance device options in the *Surveillance Devices Act 2004* available to monitor compliance with a control order subject to authorisation processes contained within the Act. The *Surveillance Devices Act 2004* does not prohibit the use of surveillance devices without a warrant in circumstances where the use of the device is lawful such as where no trespass is involved. This includes using an optical surveillance device (a camera) in public or enabling persons assisting police to record conversation to which they are a party or could be reasonably expected to overhear. Consistent with this the Bill does not require a warrant in those circumstances for the purpose of monitoring a control order.[184]

3.169 The Department also reiterated the rationale for the deferred reporting arrangements set out in the Explanatory Memorandum:

179 Law Council of Australia, *Submission 6*, p. 21.

180 Law Council of Australia, *Submission 6*, p. 21.

181 Queensland Government, *Submission 16*, p. 5.

182 Queensland Government, *Submission 16*, p. 5.

183 Attorney-General's Department, *Submission 9*, p. 9.

184 Attorney-General's Department, *Submission 9.1*, p. 23.

> Due to the generally small number of control orders likely to be in force at any one time, immediate public reporting may enable an individual to determine or speculate as to whether they are subject to covert surveillance. In turn, there is a risk that the person may modify their behaviour to defeat the surveillance efforts. Conversely, public reporting that would effectively confirm that a person is not being monitored may increase the risk that the person will breach the conditions of the order based on a belief that their actions will not be detected.[185]

3.170 The Department further explained that it considered it unnecessary to amend the Bill to allow the Queensland PIM to report on the use of surveillance device warrants in a subsequent report, stating that

> the Queensland Public Interest Monitor's annual reporting obligations relate to, in the context of control orders, the number of control orders confirmed, declared void, revoked or varied during the year, and the use of control orders generally, and in the surveillance devices context, to those issued under the aforementioned Queensland Acts. By comparison, public annual reporting on the operation of the *Surveillance Devices Act 2004* (Cth) is the responsibility of, and is undertaken by, the Commonwealth Attorney-General.[186]

Committee comment

3.171 It is critical that law enforcement has sufficient powers to use surveillance devices to determine whether an individual has complied with the conditions of their control order. This includes the ability to covertly use surveillance devices to monitor a person's compliance with controls such as restrictions or prohibitions on communicating or associating with specified individuals, accessing or using specified telecommunications or technology, and carrying out specified activities.

3.172 The Committee's views in relation to telecommunications interception powers equally apply to the surveillance device provisions, including with respect to the deferred reporting arrangements.

3.173 The Committee notes concerns from submitters regarding the transparency and accountability of the proposed regime, particularly the deferred reporting provisions. As with the TI control order warrants regime, the proposed and existing safeguards in the SD Act would be

185 Attorney-General's Department, *Submission 9.1*, p. 25.

186 Attorney-General's Department, *Submission 9.1*, pp. 25–26.

further strengthened by a requirement for the AFP to report any breaches to the Ombudsman and for the Ombudsman to report annually to the Minister regarding AFP compliance and deferred reporting (see Schedule 8 recommendations). The Committee considers that, subject to the deferred reporting arrangements, SD control order warrants should also be subject to regular parliamentary scrutiny under the comprehensive annual reporting requirements contained in the existing SD Act.

3.174 The Committee has earlier recommended a 'least interference' test to require that due regard is given to the intrusion on privacy and liberty when a monitoring warrant or TI control order warrant is issued under Schedule 8 or 9 of the Bill. The Committee notes that the issue of a SD control order warrant under Schedule 10 of the Bill will be subject to existing requirements under the SD Act that the judge or AAT member have regard to 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 sought to be obtained. Schedule 10 of the Bill also includes requirements that the judge or AAT member have regard to the likely value of the information sought to be obtained in relation to the control order monitoring purposes, and the possibility that the person has engaged, is engaging, or will engage in terrorist-related activity, or has contravened, is contravening or will contravene the control order or a succeeding control order. The Committee considers these requirements should be strengthened to include a more explicit 'least interference' test in Schedule 10.

Recommendation 14

The Committee recommends that for a surveillance device control order warrant, the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 be amended to reflect the intent of Recommendation 37 of the Council of Australian Governments Review of Counter-Terrorism Legislation, to explicitly require that:

- **the issuing officer is to have regard to whether the use of the surveillance device under the warrant constitutes the least interference with the liberty or privacy of any person that is necessary in all the circumstances.**