Chapter 2

Concluded matters

2.1 This chapter considers the responses of legislation proponents to matters raised previously by the committee. The committee has concluded its examination of these matters on the basis of the responses received.

2.2 Correspondence relating to these matters is included at **Appendix 3**.

Law Enforcement Legislation Amendment (State Bodies and Other Measures) Bill 2016

Purpose	Amends a range of legislation to reflect the establishment of the Law Enforcement Conduct Commission of New South Wales and its inspector and support its functions; to provide the Independent Broad-based Anti-corruption Commission of Victoria with investigative powers; and to amend the *Proceeds of Crime Act 2002* in respect of the meaning of lawfully acquired property or wealth
Portfolio	Attorney-General
Introduced	House of Representatives, 19 October 2016
Right	Privacy (see **Appendix 2**)
Previous report	9 of 2016

Background

2.3 The committee first reported on the Law Enforcement Legislation Amendment (State Bodies and Other Measures) Bill 2016 (the bill) in its *Report 9 of 2016*, and requested responses from the Attorney-General and Minister for Justice by 16 December 2016.[1]

2.4 The bill passed both Houses of Parliament on 24 November 2016 and received Royal Assent on 30 November 2016.

2.5 The Minister for Justice's response to the committee's inquiries, which included a response on behalf of the Attorney-General, was received on 4 January 2017. The response is discussed below and is reproduced in full at **Appendix 3**.

1 Parliamentary Joint Committee on Human Rights, *Report 9 of 2016* (22 November 2016) 2-8.

Access to communications and telecommunications data by the NSW Law Enforcement Conduct Commission

2.6 The amendments include the NSW Law Enforcement Conduct Commission (LECC) in the definition of 'eligible authority' under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and thereby permit the Attorney-General to declare the LECC to be an 'interception agency'.[2] Additionally, the LECC has been included in the definition of 'criminal law-enforcement agency' in the TIA Act. The effect of being declared an 'interception agency' and inclusion as a 'criminal law-enforcement agency' will permit LECC officers to carry out a range of activities, such as applying for a warrant to access stored communications content[3] and self-authorising access to metadata.[4]

2.7 The previous analysis noted that, as the TIA Act was legislated prior to the establishment of the committee, the scheme has never been required to be subject to a foundational human rights compatibility assessment in accordance with the terms of the *Human Rights (Parliamentary Scrutiny) Act 2011* (Human Rights Act). It was noted that the committee was therefore faced with the difficult task of assessing the human rights compatibility of permitting an agency to access powers under the TIA Act without the benefit of a foundational human rights assessment of the Act.

2.8 The previous analysis noted that the statement of compatibility identified that the measures engage the right to privacy and were stated that they were proportionate to the stated objective of providing effective frameworks to identify, investigate and punish corruption and to protect public order through enforcing the law. It was noted that this appeared to be a legitimate objective for the purposes of international human rights law, and that access to telecommunications data and communications would appear to be rationally connected to this objective.

2.9 However, as to whether the measure is proportionate to the objective being sought, the previous analysis discussed that the committee had formerly examined chapter 4 of the TIA Act,[5] and raised concerns with respect to: whether the internal self-authorisation process for access to telecommunications data by 'enforcement agencies' provided sufficient safeguards in relation to the right to privacy; accessed data subsequently being used for an unrelated purpose; and safeguards around the

2 Subject to the requirement that the respective state legislation meets the requirements in section 35 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

3 See section 109 of the TIA Act.

4 'Telecommunications data' refers to metadata rather than information that is the content or substance of a communication: see section 172 of the TIA Act.

5 In the context of its consideration of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (which amended the TIA Act) – see: Parliamentary Joint Committee on Human Rights, *Twentieth Report of the 44th Parliament* (18 March 2015) 39-74.

period of retention of such data and the absence of a warrant process.[6] It was noted that the statement of compatibility for the bill did not address these concerns.[7]

2.10 The previous analysis also identified that allowing the LECC to be declared an 'interception agency'[8] also has implications in relation to the right to privacy, and although access to private communication is via a warrant regime which itself may be sufficiently circumscribed, the use of warrants does not provide a complete answer as to whether chapters 2 and 3 of the TIA Act constitute a proportionate limit on the right to privacy.[9] It was noted that further information from the Attorney-General in relation to the human rights compatibility of the TIA Act would assist a human rights assessment of the proposed measures in the context of the TIA Act.[10]

2.11 The committee therefore sought the advice of the Attorney-General on:

- whether permitting the LECC to access such powers under the TIA Act constitutes a proportionate limit on the right to privacy (including in respect of matters previously raised by the committee); and
- whether an assessment of the TIA Act could be undertaken to determine its compatibility with the right to privacy (including in respect of matters previously raised by the committee).

Minister's response

2.12 The Minister for Justice provided the committee with the Attorney-General's response.

2.13 The Attorney-General's response stated that the Australian government considers that restricting access under the TIA Act to specified national security and law enforcement agencies 'supports both the protection of privacy and needs of criminal law-enforcement agencies given the early stage at which such disclosures are sought.'

2.14 The Attorney-General also referred to the government's previous response to the committee in respect of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Data Retention Bill), which sought to address the committee's concerns that warrantless access to telecommunications data be

6 Parliamentary Joint Committee on Human Rights, *Report 9 of 2016* (22 November 2016) 4-5.

7 Parliamentary Joint Committee on Human Rights, *Report 9 of 2016* (22 November 2016) 5.

8 Which would enable it to access the content of private communications via warrant under chapter 2 and chapter 3 of the TIA Act.

9 Parliamentary Joint Committee on Human Rights, *Report 9 of 2016* (22 November 2016) 5.

10 Parliamentary Joint Committee on Human Rights, *Report 9 of 2016* (22 November 2016) 5.

limited to certain categories of serious crimes.[11] The Attorney-General noted that self-authorisation by an officer of a criminal law-enforcement agency to access telecommunications data may only occur where:

> (1) it is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty or for the protection of the public revenue; and
>
> (2) the authorising officer of an agency is satisfied on reasonable grounds that any interference with privacy is justifiable and proportionate.

2.15 However, the Attorney-General's response does not discuss why there is no limit on the type of criminal offence being investigated for which telecommunications data can be accessed. As the committee previously noted in respect of the Data Retention Bill, the scheme allows access to metadata for the investigation of minor offences, not all of which appear to be sufficiently serious to justify the interference with the right to privacy that the scheme imposes.[12] In the case of the LECC, the Attorney-General's response stated that authorised officers will 'only be able to authorise the disclosure of data for investigations into corruption, misconduct and maladministration on the part of New South Wales law enforcement where that investigation also meets the TIA Act thresholds'.[13] However, the Attorney-General's response does not refer to the NSW legislation which establishes the LECC under the *Law Enforcement Conduct Commission Act 2016* (NSW) and the scope of the LECC's complaint handling and investigative powers under that Act. Pursuant to that Act, investigations can be carried out in respect of serious maladministration, which is defined as including that the conduct is unlawful as it constitutes 'an offence'. There does not appear to be any limit on the level of seriousness of the type of offence that could be considered to be maladministration.

2.16 The committee previously recommended in respect of the Data Retention Bill that the TIA Act limit disclosure authorisation for existing data to instances where it is reasonably necessary for the investigation of specified serious crimes, categories of serious crimes or the investigation of serious matters by the Australian Securities and Investments Commission, the Australian Taxation Office and the Australian Competition and Consumer Commission.[14] The committee considered this would

---

11 Parliamentary Joint Committee on Human Rights, *Twentieth Report of the 44th Parliament* (18 March 2015) Appendix 1 *Australian Government response to the 15th report of the Parliamentary Joint Committee on Human Rights to the 44th Parliament, Telecommunications (Interception and Access) Amendment (Data Retention) Bill* 8-10.

12 Parliamentary Joint Committee on Human Rights, *Twentieth Report of the 44th Parliament* (18 March 2015) 58.

13 See Appendix 3, letter from the Hon Michael Keenan MP, Minister for Justice, to the Hon Ian Goodenough MP (received 4 January 2017) 2.

14 Parliamentary Joint Committee on Human Rights, *Twentieth Report of the 44th Parliament* (18 March 2015) 59.

avoid the disproportionate limitation on the right to privacy that would result from disclosing telecommunications data for the investigation of *any* offence.[15] As this issue is also unaddressed by the current bill, these concerns therefore remain.

2.17 The Attorney-General also discussed other existing safeguards: that agencies, such as the LECC, are restricted by their enabling legislation; and that in its consideration of the Data Retention Bill, the majority of the committee noted that the existing requirements in the TIA Act regarding internal agency authorisation for disclosure of telecommunications data 'provide a sufficient safeguard to address privacy concerns.' It should be noted, however, that this split conclusion by the committee was confined to the committee's consideration of oversight and accountability of the mandatory data retention scheme, and not the broader issues in respect of the Data Retention Bill.[16]

2.18 The Attorney-General's response also noted that:

> [o]nce accessed, telecommunications data may only be communicated for a purpose connected with the functions of the accessing agency for the purposes of enforcing the criminal law, a law imposing a pecuniary penalty or protecting the public revenue. Both the TIA Act and the LECC's enabling legislation impose criminal liability on LECC officers who communicate information relating to the disclosure of data for unauthorised purposes.[17]

2.19 The Attorney-General's response also discussed oversight of the access to and use of telecommunications data by the Commonwealth Ombudsman. It was stated that this is an effective accountability mechanism that does not risk delaying law enforcement investigations, or harming the ability of agencies to investigate crime and safeguard national security in the way that a warrant regime, proposed by the committee in its consideration of the Data Retention Bill, would do. It was also noted that the powers within the TIA Act, which are subject to a warrant, are used in the latter stages of an investigation, and that access to telecommunications data in the first instance assists in determining who should be subject to a warrant.

2.20 The Attorney-General's response therefore concluded that 'given the existing safeguards within the Act, access to the content of private communications by the LECC is a reasonable and proportionate limitation on the right to privacy.' In respect of the committee's concerns about the absence of a warrant process, the Attorney-General concluded that:

> [a]lthough warrants may relate to a broad range of services and devices, a warrant may only be issued for the purpose of investigating specific

15 Parliamentary Joint Committee on Human Rights, *Twentieth Report of the 44th Parliament* (18 March 2015) 59.

16 Parliamentary Joint Committee on Human Rights, *Twentieth Report of the 44th Parliament* (18 March 2015) 65-71.

17 See Appendix 3, letter from the Hon Michael Keenan MP, Minister for Justice, to the Hon Ian Goodenough MP (received 4 January 2017) 3.

> offences that meet thresholds identified in the [TIA] Act and in relation to services or devices likely to be used by the target.[18]

2.21 While the response therefore discussed some of the committee's previous concerns and recommendations, the Attorney-General has not identified how the Ombudsman as an oversight mechanism (which only applies after the exercise of the power) offers comparable, adequate protections in respect of the right to privacy as a warrant process. As such, it cannot be determined that the limitation on the right to privacy is proportionate to the stated objective of the measure.

2.22 In respect of the committee's query over whether an assessment of the TIA Act could be undertaken to determine its compatibility with the right to privacy, the Attorney-General responded that, as the TIA Act was enacted before the Human Rights Act, there is no requirement that the TIA Act be subject to a human rights compatibility assessment. It was noted that the Attorney-General's Department has 'provided extensive advice regarding the operation of the TIA Act to this Committee and other Parliamentary bodies' including the committee in its consideration of the Data Retention Bill. Further, it was noted that:

> …in response to recommendation 18 of the *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* by the Parliamentary Joint Committee on Intelligence and Security in 2013, the Australian Government agreed to comprehensively revise the [TIA] Act in a progressive manner. If legislation is introduced to reform the Act, the Department will undertake a human rights compatibility assessment. The Australian Government continually reviews the TIA Act to ensure that adequate safeguards are in place to protect privacy.[19]

2.23 Despite this response, and as noted in the previous analysis, as the committee has not previously considered chapters 2 and 3 of the TIA Act in detail, further information from the Attorney-General in relation to the human rights compatibility of the TIA Act would assist a human rights assessment of the proposed measures in the context of the TIA Act.

Committee response

2.24 **The committee thanks the Attorney-General for his response and has concluded its examination of this issue.**

2.25 **The committee notes the Attorney-General's response that there is no requirement under the Human Rights Act to subject pre-existing legislation to a human rights compatibility assessment and that the Attorney-General gave no commitment to publicly undertake a human rights assessment of the TIA Act.**

---

18 See Appendix 3, letter from the Hon Michael Keenan MP, Minister for Justice, to the Hon Ian Goodenough MP (received 4 January 2017) 4.

19 See Appendix 3, letter from the Hon Michael Keenan MP, Minister for Justice, to the Hon Ian Goodenough MP (received 4 January 2017) 4.

2.26 **The committee considers that while there are certain internal and external safeguards in place in respect of the access to and subsequent use of telecommunications data, these are insufficient to protect the right to privacy for the purposes of international human rights law.**

2.27 **The committee is therefore unable to conclude that the measure, in extending access to these coercive powers to an additional body, justifiably limits the right to privacy.**

Definition of 'lawfully acquired' under the POC Act

2.28 The bill amended section 336A of the *Proceeds of Crime Act 2002* (POC Act) to provide that property or wealth is not to be considered 'lawfully acquired' where it has been subject to a security or liability that has wholly or partly been discharged using property that is not lawfully acquired. This has the effect of broadening the class of assets that may be subject to being frozen, restrained or forfeited under the POC Act.

2.29 The previous analysis noted that, as set out in the committee's *Guidance Note 2*, even if a penalty is classified as civil or administrative under domestic law, its content may nevertheless be considered 'criminal' under international human rights law. It was also noted that the committee's reports have previously raised concerns that parts of the POC Act may involve the determination of a criminal charge.[20]

2.30 Although not addressed in the statement of compatibility, the previous analysis identified that the right to be presumed innocent is engaged and limited by the measure.[21] It also identified that the forfeiture of property of a person who has already been sentenced for an offence may raise concerns regarding the imposition of double punishment;[22] and as the measure would have the effect of broadening the class of assets that may be subject to being frozen, restrained or forfeited under the POC Act, the right to a fair trial and fair hearing are engaged.[23]

2.31 The committee therefore sought the advice of the Minister for Justice on:

- whether the limitation is a reasonable and proportionate measure for the achievement of its objective (including the sufficiency of safeguards contained in the POC Act); and

---

20 Parliamentary Joint Committee on Human Rights, *Sixth Report of 2013* (15 May 2013) 189-191; and *Thirty-first Report of the 44th Parliament* (24 November 2015) 37-44.

21 Pursuant to article 14(2) of the International Covenant on Civil and Political Rights (ICCPR).

22 Contrary to article 14(7) of the ICCPR.

23 See generally, article 14 of the ICCPR.

- whether an assessment of the POC Act could be undertaken to determine its compatibility with the right to a fair trial and fair hearing in light of the committee's concerns.

Minister's response

2.32 The minister's response stated that, contrary to the committee's concern, the measure is not intended to broaden the class of assets that may be subject to being frozen, restrained or forfeited under Schedule 3 of the POC Act. The minister stated that, rather, the measure clarifies the intended meaning of the section in light of the Supreme Court of Western Australia's decision in *Commissioner of the Australian Federal Police v Huang*.[24]

2.33 However, the minister stated that if the practical effect of the amendment is to broaden the scope of assets that can be frozen, restrained or forfeited, Schedule 3 would engage the right to a fair hearing for civil hearings. As proceedings under the POC Act are heard by Commonwealth, State and Territory courts, the minister stated that such proceedings are carried out in accordance with the relevant procedures in these courts, affording affected persons adequate opportunity to present his or her case and therefore not limiting the right to a fair hearing.

2.34 The minister reiterated the government's position that 'proceeds of crime orders are classified as civil under section 315 of the POC Act and do not involve the determination of a criminal charge or the imposition of a criminal penalty.' The minister stated that, for this reason, these orders do not engage the rights set out in the International Covenant on Civil and Political Rights (ICCPR) that relate to minimum guarantees in criminal proceedings. The minister stated that as proceedings under the POC Act provide for a right to a fair hearing, the amendments do not limit the right to a fair trial under article 14 of the ICCPR.

2.35 However, as noted in the previous analysis, and as stated above, even where a penalty is classified as civil or administrative under domestic law, its content may nevertheless be considered 'criminal' under international human rights law.[25] If a measure is considered criminal for the purposes of international human rights law, it must comply with the minimum guarantees that apply in criminal proceedings, such as the right to be presumed innocent and the prohibition of double punishment.

2.36 As the committee has previously noted, 'it is clear that the POC Act provides law enforcement agencies [with] important and necessary tools in the fight against crime in Australia'.[26] If forfeiture orders are assessed as involving the determination of a criminal charge, this does not suggest that such measures cannot be taken –

24 [2016] WASC 5.

25 See Parliamentary Joint Committee on Human Rights, *Guidance Note 2* (December 2014) at Appendix 4.

26 Parliamentary Joint Committee on Human Rights, *31st Report of the 44th Parliament* (24 November 2015) 37-44 at 43-44.

rather, it requires that such measures are demonstrated to be consistent with the criminal process rights under articles 14 and 15 of the ICCPR.

2.37 The minister's response has not responded to the assessment regarding the determination of a criminal charge, or described how the measure is proportionate to the stated objective of ensuring that criminals are not able to maintain ownership over property or wealth that is obtained, either directly or indirectly, using proceeds of crime'.[27]

2.38 In respect of the committee's query over whether an assessment of the POC Act could be undertaken to determine its compatibility with the right to a fair trial and fair hearing in light of the committee's concerns, the minister stated:

> [l]egislation established prior to the enactment of the [Human Rights Act] is not required to be subject to a human rights compatibility assessment. The Australian Government continually reviews the POC Act to ensure that it addresses emerging trends in criminal conduct and will continue to undertake a human rights compatibility assessment where a Bill amends the Act.[28]

2.39 As noted in the previous analysis, in light of the committee's previously raised concerns about the sufficiency of safeguards in the POC Act to protect the right to a fair trial and the right to a fair hearing, in order to fully assess the compatibility of the proposed measures it is necessary for a detailed assessment of the POC Act in respect of these concerns to be undertaken.

Committee response

2.40 **The committee thanks the minister for his response and has concluded its examination of this issue.**

2.41 **The committee notes that the bill may have the effect of broadening the scope of assets that can be frozen, restrained or forfeited under the POC Act, and therefore expands the operation of the POC Act. The committee reiterates its earlier comments that the proceeds of crime legislation provides law enforcement agencies with important and necessary tools in the fight against crime. However, it also raises concerns regarding the right to a fair hearing and the right to a fair trial, as although a penalty is classified as civil or administrative under domestic law, its content may nevertheless be considered 'criminal' under international human rights law. The committee reiterates its previous view that the POC Act would benefit from a full review of the human rights compatibility of the legislation.**

---

27 Explanatory memorandum, statement of compatibility 13.

28 See Appendix 3, letter from the Hon Michael Keenan MP, Minister for Justice, to the Hon Ian Goodenough MP (received 4 January 2017) 5.

2.42 **Noting the preceding analysis, the committee draws the human rights implications of the provisions relating to the proceeds of crime to the attention of the Parliament.**

Privacy Amendment (Notifiable Data Breaches) Bill 2016

Purpose	Proposes to amend the *Privacy Act 1988* to impose a data breach notification requirement on entities regulated by the Act
Portfolio	Attorney-General
Introduced	House of Representatives, 19 October 2016
Rights	Privacy; effective remedy (see **Appendix 2**)
Previous report	8 of 2016

Background

2.43 The committee first reported on the Privacy Amendment (Notifiable Data Breaches) Bill 2016 (the bill) in its *Report 8 of 2016*, and requested a response from the Attorney-General by 8 December 2016.[1]

2.44 The bill remains before the House of Representatives.

2.45 The Attorney-General's response to the committee's inquiries was received on 28 November 2016. The response is discussed below and is reproduced in full at **Appendix 3**.

Accessing personal data and the right to an effective remedy

2.46 The bill seeks to impose a mandatory data breach notification requirement on entities regulated by the *Privacy Act 1988* (Privacy Act).[2] A data breach will arise where there has been unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals, or data is lost in circumstances likely to give rise to unauthorised access or disclosure. Failure to comply with these obligations is deemed to be an interference with the privacy of an individual for the purposes of the Privacy Act. The bill allows for a number of exceptions to this mandatory notification requirement.[3]

1 Parliamentary Joint Committee on Human Rights, *Report 8 of 2016* (9 November 2016) 6-8.

2 Pursuant to Schedule 1, item 3, proposed section 26WL in respect of an 'eligible data breach', as defined by section 26WE.

3 As set out in the explanatory memorandum (EM), statement of compatibility (SOC) 60-63. The exceptions address remedial action by the entity; circumstances where another entity notifies an agency of the data breach; where notification would prejudice the activities of a law enforcement body; where the Australian Information Commissioner makes a declaration for an exception; where disclosure would be inconsistent with other laws of the Commonwealth; and notification under both the bill and the *My Health Records Act 2012*.

2.47 The bill appears to address the government's intention[4] to introduce legislation to enact a mandatory data breach notification scheme.[5] In the committee's consideration of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (TIA bill) in its *Thirtieth report of the 44th Parliament*, the committee welcomed the Attorney-General's advice that such legislation would be introduced. The committee noted that, depending on the extent of the notification scheme, such a bill could address many of the committee's concerns in relation to that bill as to whether a person could seek redress in respect of breaches of their right to privacy and freedom of expression relating to the interception of their telecommunications data.

2.48 At the time, the committee also noted that it would assess any such proposed legislation in future to determine whether it addresses these concerns.[6] However, the current bill applies only to unauthorised access to, or disclosure of, personal information or data loss. It does not apply to lawful interception of telecommunications data pursuant to the *Telecommunications (Interception and Access) Act 1979* (TIA Act), which was also considered by the committee at the time.

2.49 The committee therefore sought the advice of the Attorney-General as to whether the bill could be amended to ensure that individuals are notified when their telecommunications data has been lawfully accessed (noting that there may be circumstances where such notification would need to be delayed in order to avoid jeopardising an ongoing investigation).

Attorney-General's response

2.50 In his response, the Attorney-General referred the committee to the February 2015 Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). In that report, and on the basis of concern about data breaches compromising the security of retained telecommunications data and the absence of a broad-based mandatory data breach notification requirement in Australia, the PJCIS recommended the introduction of a mandatory data breach notification scheme.

---

4 Earlier expressed to the committee in the context of the committee's consideration of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (TIA bill).

5 See Parliamentary Joint Committee of Human Rights, *Fifteenth Report of the 44th Parliament* (14 November 2014) 10-22; *Twentieth Report of the 44th Parliament* (18 March 2015) 39-74; and *Thirtieth report of the 44th Parliament* (10 November 2015) 138. The TIA bill amended the *Telecommunications (Interception and Access) Act 1979* to introduce a mandatory data retention scheme. It passed both Houses of Parliament on 26 March 2015 and received Royal Assent on 13 April 2015.

6 Parliamentary Joint Committee of Human Rights, *Thirtieth report of the 44th Parliament* (10 November 2015) 139.

2.51 The Attorney-General stated that investigations would be hampered by a requirement to notify individuals when their telecommunications data had been accessed for law enforcement or national security purposes. The Attorney-General further stated that:

> [t]he covert investigative powers contained in the Act are generally used where the integrity of an investigation would be compromised by revealing its existence.

2.52 In response to the committee's suggestion that in some circumstances notifications be delayed, the Attorney-General stated that this would carry similar risks, as:

> [i]nvestigations into serious criminality (such as counter terrorism, child exploitation or serious and organised crime) can be protracted, and would be difficult to determine when data might be appropriately disclosed. Notification, delayed or otherwise, could expose police methodologies. The existing law reflects that policy position.

2.53 In his response, the Attorney-General also referred to the 'stringent safeguards' in place in respect of lawful access to telecommunications data, including that:

- direct covert access to telecommunications data is limited to a defined set of law enforcement and security agencies and authorised officers within those agencies will only disclose such data where it is 'reasonably necessary for the enforcement of criminal law, a law imposing a pecuniary penalty or the protection of the public revenue';
- the Australian Security Intelligence Organisation may authorise access to telecommunications data for the performance of its functions, subject to a statutory requirement that an authorising officer must be satisfied on reasonable grounds that any interference with privacy is justifiable and proportionate; and
- agency access is subject to oversight by the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security.

2.54 The committee has previously stated that, in the context of the accessing of telecommunications data, the right to an effective remedy would be supported by a notification requirement. This is because, for example, it would be impossible for an individual to seek redress for breach of their right to privacy if they did not know that data pertaining to them had been subject to an access authorisation.[7] It is noted that this bill, in applying only to unauthorised access to, or disclosure of, personal information or data loss, does not apply to lawful interception of telecommunications data pursuant to the TIA Act. As such, this bill does not address

7 See Parliamentary Joint Committee on Human Rights, *Twentieth report of the 44th Parliament* (18 March 2015) 39-74 at 73.

the committee's previous concerns in relation to the TIA bill as to whether a person could seek redress in respect of breaches of their right to privacy and freedom of expression relating to the interception of their telecommunications data.

2.55 However, the bill itself, as noted in the initial human rights analysis, does broadly promote the right to privacy and is likely to be compatible with international human rights law.

Committee response

2.56 **The committee thanks the Attorney-General for his response and has concluded its examination of this issue.**

2.57 **The committee notes that the bill promotes the right to privacy. The committee notes that the bill does not address the committee's previous concerns in relation to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 as it applies only to unauthorised access to, or disclosure of, personal information or data loss and does not apply to the lawful interception of telecommunications data.**

Sex Discrimination Amendment (Exemptions) Regulation 2016 [F2016L01445]

Purpose	Amends the Sex Discrimination Regulations 1984 to extend for a further 12-month period the prescription of two Western Australian Acts as exempt under the *Sex Discrimination Act 1984*, with the effect that an exemption would be provided for conduct taken in direct compliance with these Acts that would otherwise constitute unlawful discrimination on the grounds of sexual orientation, gender identity or intersex status
Portfolio	Attorney-General
Authorising legislation	*Sex Discrimination Act 1984*
Last day to disallow	1 December 2016
Right	Equality and non-discrimination (see **Appendix 2**)
Previous report	9 of 2016

Background

2.58 The committee first reported on the instrument in its *Report 9 of 2016*, and requested a response from the Attorney-General by 16 December 2016.[1]

2.59 The Attorney-General's response to the committee's inquiries was received on 21 December 2016. The response is discussed below and is reproduced in full at **Appendix 3**.

Extension of prescription period

2.60 Section 5 of the Sex Discrimination Regulations 1984 (the regulations) provided that all Commonwealth, state and territory laws as in force at 1 August 2013 were initially prescribed by the regulations as exempt from complying with provisions of the *Sex Discrimination Act 1984* prohibiting discrimination on the grounds of sexual orientation, gender identity of intersex status until 31 July 2014. This was to allow time for jurisdictions to review their laws and assess compliance with the new protections against these forms of discrimination, and provide protections against discrimination for same-sex de facto couples which were introduced in 2013.[2]

1 Parliamentary Joint Committee on Human Rights, *Report 9 of 2016* (22 November 2016) 27-29.

2 The amendments to the *Sex Discrimination Act 1984* that introduced these new protections were made by the *Sex Discrimination Amendment (Sexual Orientation, Gender Identity and Intersex Status) Act 2013*.

2.61 The Sex Discrimination Amendment (Exemptions) Regulation 2014 extended the sunset date applying to the prescription of state and territory laws for a 12-month period to 31 July 2015. The Sex Discrimination Amendment (Exemptions) Regulation 2015 then extended this for a further 12 month period until 31 July 2016.

2.62 The Sex Discrimination Amendment (Exemptions) Regulation 2016 (the regulation) has now extended the prescription of two Western Australian Acts (WA Acts); the *Human Reproductive Technology Act 1991* (WA), and *Surrogacy Act 2008* (WA), for a further 12-month period until 31 July 2017.

2.63 As the regulation further extends the period in which actions that would otherwise constitute unlawful discrimination under the prescribed legislation would be exempted from these protections, the committee noted that the measure engages and limits the right to equality and non-discrimination. The committee identified that questions arise as to whether this measure is rationally connected and/or proportionate to this stated objective.

2.64 The committee therefore sought the advice of the Attorney-General as to whether the further 12-month prescription period in respect of the WA Acts is effective in achieving and/or proportionate to its apparent objective, and in particular, why the previous three-year period has been insufficient to implement the necessary amendments to these laws to ensure compliance with the protections against discrimination on the basis of a person's sexual orientation, gender identity and intersex status.

Attorney-General's response

2.65 In his response, the Attorney-General stated that the Western Australian Government indicated the further extension of time was required to facilitate the amendment of the two WA Acts.[3]

2.66 The Attorney-General stated that while the government does not consider that a state should continue to discriminate against people on the basis of their sexual orientation, gender identity and/or intersex status, the government:

> …acknowledges that the regulation of assisted reproductive technology and surrogacy is a sensitive issue that is primarily a matter for states and territories and that the Western Australian government should be granted additional time to properly consult the Western Australian community about options for reform in this area.

3 The Attorney-General identified that section 23 of the *Human Reproductive Technology Act* (WA) has the effect of prohibiting male same-sex couples, and potentially transgender persons or persons of intersex status, from accessing IVF procedures-including for the purpose of a surrogacy arrangement; and that section 19 of the *Surrogacy Act* (WA) has the effect of prohibiting male same-sex couples, and potentially transgender persons or persons of intersex status, from seeking a parentage order for a child born under a surrogacy arrangement.

2.67 The Attorney-General stated that the limitation is proportionate on the basis that it allows a 'sufficient yet not overly lengthy time' for the Western Australian Government to properly consult with the Western Australian community on options for reform to its legislation. The Attorney-General noted that the Western Australian Government has advised that it does not propose any further extensions of this exemption after 31 July 2017.

2.68 However, the response does not indicate why the preceding three-year period has been inadequate to perform such consultation. As noted in the previous human rights analysis, at the end of the extended prescription period on 31 July 2017, the two WA Acts will have been exempted for a total of four years since the measures came into effect, preventing individuals who may continue to be subject to discrimination under these WA Acts from accessing legal recourse.

2.69 As noted in the previous human rights analysis, continuing to subject individuals to discriminatory laws for any length of time is a serious issue from the perspective of the right to equality and non-discrimination.

Committee response

2.70 **The committee thanks the Attorney-General for his response and has concluded its examination of this issue.**

2.71 **As the committee previously acknowledged, the measure appears to pursue the apparent objective of allowing states and territories adequate time in which to review their legislation and assess compliance with the new protections, and amend relevant laws accordingly.**

2.72 **While continuing to subject individuals to discriminatory laws for any length of time is a serious issue from the perspective of the right to equality and non-discrimination, the committee notes the Attorney-General's response that more time is needed to allow consultation on options for reform and that no extension after 31 July 2017 is proposed.**

Mr Ian Goodenough MP

Chair