Investigation and Prosecution Measures Bill 2017

Purpose	Seeks to amend the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004* to reflect a restructuring of the Independent Commission Against Corruption of New South Wales. Also seeks to amend the *Director of Public Prosecutions Act 1983* to extend the functions, powers and duties of the Commonwealth Director of Public Prosecutions to the laws of Norfolk Island
Portfolio	Attorney-General
Introduced	House of Representatives, 13 September 2017
Right	Privacy (see **Appendix 2**)
Status	Advice only

Background

1.281 The committee has previously considered proposed amendments to the *Telecommunications (Interception and Access) Act 1979* (TIA Act).[1] The committee has also previously considered proposed amendments to the *Surveillance Devices Act 2004* (SD Act).[2]

1.282 As both Acts were legislated prior to the establishment of the committee, neither has been subject to a foundational human rights compatibility assessment in accordance with the *Human Rights (Parliamentary Scrutiny) Act 2011*. As the committee has previously noted in relation to the TIA Act,[3] it is difficult to assess the

1 See, Parliamentary Joint Committee on Human Rights, Law Enforcement Integrity Legislation Amendment Bill 2012, *Fifth Report of 2012* (October 2012) 21-21; Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, *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) 133-139; the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015, *Thirty-second report of the 44th Parliament* (1 December 2015) 3-37 and *Thirty-sixth report of the 44th Parliament* (16 March 2016) 85-136; the Law Enforcement Legislation Amendment (State Bodies and Other Measures) Bill 2016, *Report 9 of 2016* (22 November 2016) 2-8 and *Report 1 of 2017* (16 February 2017) 35-44; and the Telecommunications (Interception and Access - Law Enforcement Conduct Commission of New South Wales) Declaration 2017 [F2017L00533], *Report 7 of 2017* (8 August 2017) 30-33.

2 See, Parliamentary Joint Committee on Human Rights, Counter-Terrorism Legislation Amendment Bill (No. 1) 2015; *Thirty-second report of the 44th Parliament* (1 December 2015) 3-37 and *Thirty-sixth report of the 44th Parliament* (16 March 2016) 85-136.

3 Parliamentary Joint Committee on Human Rights, Law Enforcement Legislation Amendment (State Bodies and Other Measures) Bill 2016, *Report 9 of 2017* (22 November 2016) 2-8.

human rights compatibility of measures which extend or amend existing legislation without the benefit of a foundational human rights assessment.

Access to communications and telecommunications data and surveillance device warrants by the NSW Independent Commission Against Corruption

1.283 The TIA Act provides a legislative framework that criminalises the interception and accessing of telecommunications. However, the TIA Act sets out exceptions that enable defined or declared agencies to apply for access to communications[4] and telecommunications data.[5] Chapters 2 and 3 of the TIA Act provide for warranted access by an agency to the content of communications, including both communications passing across telecommunications services[6] and stored communications content. Chapter 4 of the TIA Act provides for warrantless access to telecommunications data (metadata) by a defined or declared 'interception agency'. The TIA Act vests certain positions within these agencies with specific authority.

1.284 The SD Act governs the use of optical surveillance devices, listening devices, data surveillance devices and tracking devices by law enforcement agencies. The SD Act permits certain law enforcement agencies to obtain surveillance device warrants. The SD Act also vests certain positions within these agencies specific authority when undertaking functions under the SD Act.[7]

1.285 The Independent Commission Against Corruption of New South Wales (the ICAC) has previously been declared as an 'interception agency' for the purposes of the TIA Act and is also included in the definition of 'criminal law enforcement agency' under the TIA Act. This means that the ICAC can apply for interception warrants and access telecommunications data under the TIA Act.

1.286 The bill seeks to amend the TIA Act to reflect a restructuring of the ICAC under the *Independent Commission Against Corruption Amendment Act 2016* (NSW).[8] That is, it amends which positions within the ICAC are vested with specific authority and powers under the TIA Act. Specifically, the bill amends the definition of

---

4 'Communication' is defined in section 5 of the TIA Act as including: 'conversation and a message, and any part of a conversation or message, whether: (a) in the form of: (i) speech, music or other sounds; (ii) data; (iii) text; (iv) visual images, whether or not animated; or (v) signals; or (b) in any other form or in any combination of forms'.

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

6 That is, the interception of live communications.

7 Explanatory Memorandum (EM) 3.

8 The restructured commission consists of a chief commissioner, two commissioners and, as required, assistant commissioners, replacing the former structure of a commissioner and assistant commissioners. See EM 2.

'certifying officer' as it relates to the ICAC under the TIA Act to refer to the ICAC's current structure of a 'chief commissioner', a 'commissioner' or an 'assistant commissioner'. The bill also seeks to replace references in the TIA Act to the ICAC's 'commissioner' with the 'chief commissioner', including as it relates to the definition of 'chief officer' under the TIA Act.[9] For example, the 'chief officer' has the authority to empower members of the ICAC to receive information obtained under warrants and communicate intercepted information to other agencies in specific circumstances.[10]

1.287 Similarly, the bill seeks to amend the definition of 'chief officer' as it relates to the ICAC under the SD Act to refer to the 'chief commissioner' of a 'law enforcement agency'. The bill also seeks to amend the definition of 'authorising officer' under the SD Act to refer to the ICAC's 'chief commissioner', a 'commissioner' or an 'assistant commissioner'. 'Authorising officers' will for example have the power to issue emergency authorisations for the use of a surveillance device and authorise the use and retrieval of tracking devices without warrant in certain circumstances.[11]

Compatibility of the measure with the right to privacy

1.288 The right to privacy includes the right to respect for private and confidential information, particularly the storing, use and sharing of such information and the right to control the dissemination of information about one's private life. As the bill relates to the ICAC's powers to access an individual's private communications and telecommunications data as well as obtaining surveillance of an individual's private life through the use of devices the bill engages and limits the right to privacy.

1.289 A limitation on the right to privacy will be permissible under international human rights law where it addresses a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

1.290 The statement of compatibility acknowledges that the bill engages the right to privacy and identifies the broader objective of the measures as preventing criminal activity 'by ensuring that law enforcement and intelligence agencies have access to communications and associated information central to virtually every organised crime, counter espionage, cyber security and counter-terrorism investigation'.[12] In general terms these may be capable of constituting a legitimate objective for the purposes of international human rights law. Vesting particular positions within the ICAC with specific authority when undertaking functions under the SD Act and the TIA Act and enabling access to telecommunications and communications data would also appear to be rationally connected to this objective.

---

9 See subsection 5(1) (paragraph (e), TIA Act.

10 See EM 3.

11 EM 3.

12 EM, statement of compatibility (SOC) 7.

1.291 As to the proportionality of accessing certain communications content, the statement of compatibility explains the operation of warrants as a relevant safeguard:

> Interception of telecommunications and access to stored communications may only occur subject to a warrant issued by an independent issuing authority (a judge or member of the Administrative Appeals Tribunal). When deciding whether a warrant should be issued the issuing authority must have regard to several factors, including: the privacy impacts; the gravity of the offence; the extent to which other investigative methods are available, and the likely usefulness of the information to the relevant investigation...[13]

1.292 As the committee has previously noted in its consideration of measures enabling agencies to access powers under the TIA Act,[14] although access to private communications 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. The committee has previously noted that, as it had 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 proposed measures that amend or extend the Act.

1.293 In relation to the proportionality of authorised officers permitting access to telecommunications data (metadata), the statement of compatibility argues:

> Authorised officers are required to consider similar factors before authorising the disclosure of telecommunications data. Authorised officers must be satisfied that the disclosure of telecommunications data is reasonably necessary for the enforcement of the criminal law, protection of the public revenue or for the enforcement of a law imposing a pecuniary penalty and that any interference with the privacy of any person is justifiable and proportionate.[15]

1.294 The committee has also previously raised concerns in relation to this warrantless access to telecommunications data (metadata) under chapter 4 of the TIA Act. This included: whether the internal self-authorisation process for access to

---

13 EM, SOC 6.

14 See, Parliamentary Joint Committee on Human Rights, Telecommunications (Interception and Access - Law Enforcement Conduct Commission of New South Wales) Declaration 2017 [F2017L00533], *Report 7 of 2017* (8 August 2017) 30-33. This instrument declared the Law Enforcement Conduct Commission of New South Wales an interception agency for the purposes of the TIA Act. Also see: Law Enforcement Legislation Amendment (State Bodies and Other Measures) Bill 2016, *Report 1 of 2017* (16 February 2017) 35-44.

15 EM, SOC 6.

telecommunications data by prescribed agencies contains sufficient safeguards; accessed data subsequently being used for an unrelated purpose; and safeguards in relation to the period of retention of such data.[16] In its examination of legislation declaring the Law Enforcement Conduct Commission of New South Wales an 'interception agency' and a 'criminal law enforcement agency' under the TIA Act — the same standing under the TIA Act as the Independent Commission Against Corruption of New South Wales — the committee determined that while there were certain internal and external safeguards in place in respect of the access to and subsequent use of telecommunications data, these were insufficient to protect the right to privacy for the purposes of international human rights law.[17]

1.295 As these concerns in relation to the powers vested in declared and defined agencies under the TIA Act remain unresolved, it cannot be determined that the limitation on the right to privacy in the bill is proportionate to the stated objective. The absence of a foundational assessment of the SD Act may also raise similar concerns.

Committee comment

1.296 Consistent with its previous reports in relation to the powers granted to particular agencies to access communications and telecommunications data under the *Telecommunications (Interception and Access) Act 1979*, the committee is unable to conclude that the bill justifiably limits the right to privacy.

1.297 The committee considers that the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004* would benefit from a full review of their compatibility with the right to privacy, including the sufficiency of safeguards.

1.298 Noting the human rights concerns regarding the right to privacy identified in its previous reports, the committee draws the human rights implications of the bill to the attention of the parliament.

16 Parliamentary Joint Committee on Human Rights, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Fifteenth Report of the 44th Parliament (November 2014) 10 – 22; *Twentieth report of the 44th Parliament* (18 March 2015) 39-74 and Law Enforcement Legislation Amendment (State Bodies and Other Measures) Bill 2016, *Report 1 of 2017* (16 February 2017) 36.

17 Parliamentary Joint Committee on Human Rights, *Report 1 of 2017* (16 February 2017) 41.