Appendix 3

Correspondence

THE HON MICHAEL KEENAN MP
Minister for Justice
Minister Assisting the Prime Minister for Counter-Terrorism

MS16-018127

Chair
Parliamentary Joint Committee on Human Rights
Sl.111
Parliament House
CANBERRA ACT 2600
<human.rights@aph.gov.au>

Dear Chair

I refer to the letter from the Committee Secretary of the Parliamentary Joint Committee on Human Rights (the Committee) dated 23 November 2016. This letter brought to my attention the comments contained in the Committee' *Report 9 of 2016*. In this Report, the Committee identified a number of human rights compatibility issues with the Law Enforcement Legislation Amendments (State Bodies and Other Measures) Bill 2016 (the Bill).

I have consulted the Attorney-General, Senator the Hon George Brandis QC, in providing the below response

Compatibility of measures in Schedule 1

The committee requests the further advice of the Attorney-General as to:

> *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).*

Attorney-General's response

Right to privacy

The provisions in Schedule 1 of the Act engage the right to privacy under Article 17 of the ICCPR. To the extent that Schedule 1 limits the right to privacy, these limitations are not arbitrary and are necessary, reasonable and proportionate to the achievement of the legitimate objective of enabling the Law Enforcement Conduct Commission (LECC) to identify, investigate and punish corruption.

Limitations on access to and use of telecommunications data

The Committee has raised concerns about:

(a) the broad nature of telecommunications data authorisations

(b) the ability to subsequently use such information, and

(c) whether the internal self-authorisation process for access to data provides sufficient safeguards in relation to the right to privacy.

Telecommunications data is critical to the investigation of criminal activity, including corruption investigations, and is used at the early stages of investigations to build a picture of a target and the target's network of associates. Access under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) is limited to specified national security and law enforcement agencies (of which the LECC is replacing an existing body). The Australian Government considers restricting access to specified agencies supports both the protection of privacy and needs of criminal law-enforcement agencies given the early stage at which such disclosures are sought. The Australian Government has previously provided a response addressing concerns that access to data be limited to certain categories of serious crimes.[1]

There is a two-fold test that must be met before an officer of a criminal law-enforcement agency may authorise the disclosure of data. Disclosure 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]

Agencies are further restricted by their enabling legislation. In the case of the LECC, 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. As discussed below, any further restrictions (such as the requirement to apply for a warrant to access data) would fundamentally undermine the utility of data as an investigative tool.

The internal safeguard provisions were previously considered as a part of the Parliamentary Joint Committee on Human Rights, *Twentieth Report of the 44th Parliament* in March 2015. At this time, the Committee considered the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 and the majority of the Committee observed that existing requirements for internal agency authorisations provided sufficient safeguards to address privacy concerns.[3]

---

[1] 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.

[2] This requirement was included in response to a recommendation from the Parliamentary Joint Committee on Intelligence and Security *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (February 2015) 251.

[3] Parliamentary Joint Committee on Human Rights, *Twentieth Report of the 44th Parliament* (18 March 2015) at [1.237].

Once 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.

Oversight through a warrant process or the Commonwealth Ombudsman

Access to and use of telecommunications data is subject to stringent reporting requirements and independent oversight by the Commonwealth Ombudsman. New record-keeping and reporting obligations introduced through the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* increase transparency of the use of telecommunications data by criminal law enforcement agencies.

The LECC will be required to keep comprehensive records to assist the Ombudsman in its inspection of the access and use of data by the agency. The Ombudsman has extensive powers under the TIA Act to compel the disclosure of information relating to agency activities. Furthermore, agencies are now required to report annually on the:

- types of data accessed in investigations,
- length of time data was retained by the service provider prior to an authorisation by an agency, and
- type of offences investigated with the use of data.

Both the Ombudsman's report and TIA Act annual report will be tabled in Parliament each year to enable public scrutiny.

The Australian Government considers that introducing a warrant regime for telecommunications data to augment existing safeguards would risk serious harm to the ability of agencies to investigate crime and safeguard national security. Warrant applications are lengthy processes and telecommunications data is commonly used at the early stages of an investigation, when delays can result in the loss of evidence. Current arrangements, such as external oversight by the Commonwealth Ombudsman, serve as an effective accountability mechanism without delaying law enforcement investigations. In addition, an oversight body has the advantage of reviewing how an agency has accessed and used telecommunications data from end-to-end.

Finally, the powers within the TIA Act which are subject to a warrant are used in the latter stages of an investigation. Access to telecommunications data often provides foundational information commonly used to exclude others from suspicion, ensuring they are not targeted by more intrusive investigative techniques such as telecommunications interception or surveillance (which require a warrant). Accordingly, there is a clear distinction between the privacy impact of access to telecommunications data and the execution of a telecommunications interception warrant. Further detail on this distinction can be found in the February 2015 response the Australian Government supplied addressing a previous recommendation from the Committee that access to data be subject to a warrant process.[4]

[4] 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* 12-14. .

Access to content of communications given the services and devices which can be impacted

The Australian Government considers 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. Before the LECC, or any eligible agency, is able to access the content of private communications it must apply to an independent issuing authority for a warrant. Issuing authorities are required to consider the proportionality of the agency's request in every instance, including how the privacy of any person may be impacted.

Although warrants may relate to a broad range of services and devices, a warrant may only be issued for the purpose of investigating specific offences that meet thresholds identified in the Act and in relation to services or devices likely to be used by the target. Interception warrants may only be obtained to assist in the investigation of defined serious offences, generally attracting a maximum penalty of at least seven years imprisonment for interception warrants or offences of at least three years imprisonment for access to stored communications. Similar to the oversight arrangements for telecommunications data, the Commonwealth Ombudsman and state oversight bodies inspect and report on agency access to private communications to ensure law enforcement agencies exercise their authority appropriately.

The measures within Schedule 1 broadly engage the right to privacy. However, the safeguards within the TIA Act discussed above ensure that any limitations on that right are reasonable, necessary and proportionate to the legitimate goals of promoting accountability in law enforcement, investigating corruption and protecting public order through enforcing the law.

Assessment of the TIA Act

Legislation established prior to the enactment of the *Human Rights (Parliamentary Scrutiny) Act 2011* is not required to be subject to a human rights compatibility assessment. However, the Attorney-General's Department has provided extensive advice regarding the operation of the TIA Act to this Committee and other Parliamentary bodies. The privacy implications of the TIA Act were discussed in detail in Government responses to the Committee's scrutiny of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

Further, 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 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.

The relevant contact in the Attorney-General's Office is Timothy Roy who can be contacted on 6277 7300.

Compatibility of measures in Schedule 3

The committee seeks the advice of the minister as to:

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

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

Right to a fair trial and fair hearing

The Committee has stated that Schedule 3, which amends the definition of 'lawfully acquired' under section 336A of the *Proceeds of Crime Act 2002* (the POC Act), broadens the class of assets that can be frozen, restrained or forfeited, limiting the right to a fair trial and hearing under Article 14 of the International Covenant on Civil and Political Rights (ICCPR).

Schedule 3, however, is not intended to broaden the scope of section 336A, but instead clarifies the intended meaning of section 336A in light of the Supreme Court of Western Australia's decision in *Commissioner of the Australian Federal Police v Huang* [2016] WASC 5.

If Schedule 3 has the practical effect of broadening the scope of assets that can be frozen, restrained or forfeited under a proceeds of crime order, this Schedule will engage the right to a fair hearing for civil hearings under Article 14(1) of the ICCPR. This right guarantees equality before courts and tribunals, and, in the determination of criminal charges, or any suit at law, the right to a fair and public hearing before a competent, independent and impartial court or tribunal established by law. Proceedings under the POC Act are proceedings heard by Commonwealth, State and Territory courts in accordance with relevant procedures of those courts. This affords an affected person adequate opportunity to present his or her case, such that the right to a fair hearing is not limited.

The Australian Government reiterates 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. These orders therefore do not engage the rights in Articles 14(2)-(7) of the ICCPR relating to minimum guarantees in criminal proceedings. As proceedings under the POC Act provide for a right to a fair hearing consistent with Article 14(1), the items under Schedule 3 do not limit the right to a fair trial under Article 14.[5]

Assessment of the POC Act

The Committee has requested that I engage in a detailed assessment of the POC Act to determine its compatibility with the right to a fair trial and a fair hearing. Legislation established prior to the enactment of the *Human Rights (Parliamentary Scrutiny) Act 2011* 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.

The relevant contact in my office for this matter is Talitha Try, who can be contacted on 6277 7290.

I trust this information has been of assistance.

Yours sincerely

Michael Keenan

[5] See Parliamentary Joint Committee on Human Rights *Thirty-first Report of the 44th Parliament* (24 November 2015) 39-42.

ATTORNEY-GENERAL

CANBERRA

MS16-018150

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
PO Box 6100
Parliament House
CANBERRA ACT 2600

Dear Chair Ian

I am writing in response to the letter from the Committee Secretary of the Parliamentary Joint Committee on Human Rights, Ms Toni Dawes, dated 9 November 2016. The letter refers to the Committee's *Report 8 of 2016* and seeks my advice in relation to whether the Privacy Amendment (Notifiable Data Breaches) Bill 2016 could be amended to require notification to individuals following access to their telecommunications data under the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

In February 2015, the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (the Advisory Report) recommended the introduction of a mandatory data breach notification scheme. The PJCIS' recommendation was based on 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 Government's response to the Advisory Report on 3 March 2015 supported this recommendation. Consistent with the Government's response, the Bill would introduce a data breach notification requirement following unauthorised access to, unauthorised disclosure of or loss of, personal information that would cause a likely risk of serious harm to individuals. The notification requirement would apply to data breaches of this kind involving telecommunications data retained by service providers under the TIA Act. However, lawful access to retained telecommunications data by law enforcement and security agencies under the Act would not fall within the Bill's notification requirement.

If individuals were notified when their telecommunications data is accessed for law enforcement or national security purposes it would hamper investigations. The covert investigative powers contained in the Act are generally used where the integrity of an investigation would be compromised by revealing its existence. The Committee's suggestion that, in some circumstances, notifications be delayed would carry similar risks. Investigations 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. It is an offence to disclose the existence of an authorisation for the access to telecommunications data under Division 6 of Part 4-1 of Chapter 4 of the Act.

Lawful access to telecommunications data is subject to stringent safeguards. Direct covert access to telecommunications data is limited to a defined set of law enforcement and security agencies. Authorised officers within those agencies may only allow the disclosure of telecommunications data where 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. The Act requires that the authorising officer be satisfied on reasonable grounds that any interference with privacy is justifiable and proportionate. Agency access is also subject to comprehensive independent oversight by the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security.

The responsible adviser for this matter in my Office is Jules Moxon who can be contacted on 02 6277 7300.

Thank you again for writing on this matter.

Yours faithfully

(George Brandis)

ATTORNEY-GENERAL

MC16-143309

CANBERRA

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
S1.111
Parliament House
CANBERRA ACT 2600
<human.rights@aph.gov.au>

21 DEC 2016

Dear Mr Goodenough

Thank you for the letter of 23 November 2016 in relation to Report 9 of 2016, in which the Parliamentary Joint Committee on Human Rights sought comment on the Privacy Amendment (Re-identification Offence) Bill 2016 andf the Sex Discrimination Amendment (Exemptions) Regulation 2016. My response to the issues raised by the committee is set out below.

Sex Discrimination Amendment (Exemptions) Regulation 2016

The committee notes that the exemption from protections against discrimination on the basis of a person's sexual orientation, gender identity and intersex status engages and limits the right to equality and non-discrimination. The committee requests advice on whether extending the exemption for two Western Australian laws for a further 12 month period is effective and proportionate in achieving the stated objective of allowing states and territories adequate time to review their legislation and assess compliance with the new protections, particularly in light of the fact that an exemption has already been in place for a previous three-year period.

Western Australia indicated that a further extension of time was required to facilitate the amendment of the *Human Reproductive Technology Act* (WA) and *Surrogacy Act* (WA). Section 23 of the Human Reproductive Technology Act 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. Section 19 of the Surrogacy Act 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.

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. However, 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.

The limitation is proportionate, allowing a sufficient yet not overly lengthy time for Western Australia to properly consult on options for reform to its legislation The Government has advised the Western Australia government that it does not propose any further extensions of this exemption after 31 July 2017.

I trust this information will assist you in concluding your consideration of this legislation.

Yours faithfully

(George Brandis)

Cc: <human.rights@aph.gov.au>