Australian Government
Office of the Australian Information Commissioner

www.oaic.gov.au
GPO Box 5218 Sydney NSW 2001
P +61 2 9284 9800 F +61 2 9284 9666
E enquiries@oaic.gov.au
Enquiries 1300 363 992 TTY 1800 620 241
ABN 85 249 230 937

Our reference: D2017/010814

Mr Andrew Hastie MP
Chair
Parliamentary Joint Committee on Intelligence and Security
Parliament House
Canberra ACT 2600

Dear Mr Hastie

Parliamentary Joint Committee on Intelligence and Security review of national security bills

I welcome the opportunity to comment on the following Bills, under review by the Parliamentary Joint Committee on Intelligence and Security:

- National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (the Espionage and Other Offences Bill)
- Foreign Influence Transparency Scheme Bill 2017 (the Foreign Influence Bill).

By way of overall comment, I recognise the important objectives of these Bills, which include protecting national security interests. At the same time, any proposals to expand agencies' powers to meet these objectives must be developed with a view to accommodating contemporary community expectations about the handling of personal information, as reflected in the *Privacy Act 1988* (the Privacy Act) and guidance issued by my Office.

Australia's privacy laws recognise that the protection of individuals' privacy, through the protection of their personal information, cannot be an absolute right. In some circumstances, privacy rights must necessarily give way where there is a compelling public interest reason to do so.[1] However, proposals that limit the right to privacy should be reasonable, necessary and proportionate, having regard to the objectives they seek to achieve.[2] My comments about these Bills focus on ensuring that any impacts on privacy are considered to be necessary, reasonable and proportionate in the circumstances.

[1] The objects of the Privacy Act include to implement Australia's international obligation in relation to privacy, as enshrined in Article 17 of the International Covenant on Civil and Political Rights (the ICCPR), available at http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[2] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc A/HRC/27/37 (2014), paragraph 23.

In particular, I suggest that:

- additional information be included in the Explanatory Memorandum (EM) to the Espionage and Other Offences Bill, to explain how the expanded definition of 'serious offence' in the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) is reasonable, necessary and proportionate, given the likely impact of this expanded definition on individuals' privacy
- a note be inserted into the Espionage and Other Offences Bill or additional information be included in the EM to the Bill, to clarify that the secrecy provisions are not intended to impact on Australian Privacy Principle (APP) 12 and the Privacy Act, including the Notifiable Data Breaches (NDB) scheme
- a privacy impact assessment (PIA) be undertaken, if one has not been already, on the registration scheme established under the Foreign Influence Bill, to identify the impact that the scheme might have on the privacy of individuals, and to set out recommendations for managing, minimising or eliminating that impact
- where a provision authorising or requiring the collection, use or disclosure of personal information is discretionary or includes a rule-making power, as under the Foreign Influence Bill, consideration be given to setting out further detail in primary legislation or requiring consultation, including with the Information Commissioner, on the development of rules.

My Office has also reviewed the Home Affairs and Integrity Agencies Legislation Amendment Bill 2017, also before the Committee. I understand from the Statement of Compatibility with Human Rights in the EM to the Bill, that this Bill engages the right to privacy in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) by authorising disclosures of AUSTRAC information by ASIO, ONA and defence intelligence agency officials to the Attorney-General.[3] As I understand, these amendments will enable the Attorney-General to retain certain existing functions when administration of the ASIC Act and TIA Act transfers to the Minister for Home Affairs, consequently I do not make comments on this Bill.

About the Office of the Australian Information Commissioner (OAIC)

The Office of the Australian Information Commissioner (OAIC) is an independent Commonwealth statutory agency. The OAIC was established by the Australian Parliament to bring together three functions:

- privacy functions (protecting the privacy of individuals' personal information under the Privacy Act and other Acts)
- freedom of information functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (the FOI Act)
- information management functions (as set out in the *Information Commissioner Act 2010*).

[3] Paragraphs 15 – 19 of the Statement of Compatibility with Human Rights

My Office also has certain powers and obligations in regards to the administration of the *Telecommunications Act 1997* and the TIA Act, including oversight of telecommunications carriers and carriage service providers' handling of telecommunications data collected under the data retention scheme in the TIA Act, which is deemed to be personal information within the meaning of the Privacy Act.

The integration of these interrelated functions into one agency has made the OAIC well placed to strike an appropriate balance between promoting the right to privacy and broader information policy goals.

National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017

Telecommunications interception and access

I understand that Schedule 2 of the Espionage and Other Offences Bill would insert a suite of new Commonwealth secrecy offences into the *Criminal Code Act 1995*, replacing the current secrecy offence provisions in sections 70 and 79 of the *Crimes Act 1914*. Schedule 3 would introduce a new aggravated offence that applies where a person provides false or misleading information in relation to an Australian Government security clearance process. Schedule 4 would add these offences to the definition of 'serious offence' in s 5D the TIA Act.

By amending s 5D of the TIA Act, the Espionage and Other Offences Bill would extend the application of the interception and access provisions of the TIA Act to new offences, [4] including to the expanded Commonwealth secrecy offences in Schedule 2 of the Bill and the new aggravated offence for giving false or misleading information in Schedule 3. This would in turn result in an increase in the circumstances where personal information may be collected, accessed and disclosed under the interception and access provisions of the TIA Act.

In some circumstances, privacy protections necessarily give way where there is a compelling public interest reason to do so. However, consistent with Article 17 of the ICCPR,[5] proposals that limit existing privacy protections, such as by expanding the circumstances in which personal information may be handled, should be demonstrably reasonable, necessary and proportionate, having regard to the policy objectives they seek to achieve.[6]

While the EM to the Espionage and Other Offences Bill considers the right to privacy and the impacts of the interception regime on this right, this consideration appears focussed on the offences created under Schedule 1 of the Bill, and concludes that 'the limitation on the right to privacy is reasonable, necessary and proportionate to achieve the legitimate objective of

---

[4] Chapters 2 and 4 of the TIA Act, respectively.

[5] The right to privacy is protected at Article 17 of the ICCPR, which states that (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; (2) Everyone has the right to the protection of the law against such interference or attacks.

[6] The Office of the United Nations High Commissioner for Human Rights, notes that to the extent that there is a restriction on an individual's right to privacy, any interference must be 'necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available' (in The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (2014), paragraph 23.)

assisting of ensuring the protection of Australia's national security.'[7] However, the EM does not make clear the need for expanding the interception and access regime under the TIA Act to include the secrecy of information offences (Schedule 2) and the aggravated false or misleading information offences (Schedule 3). If it is the intent that the interception and access regime would only be used in connection to these offences where there was a national security objective, then this should be prescribed in the Bill or explained in the EM.

Interactions with the Privacy Act and the FOI Act

As noted above, Schedule 2 of the Espionage and Other Offences Bill creates a range of new secrecy offences, which will apply if the information disclosed is inherently harmful (such as security classified information) or would otherwise cause harm to Australia's interests.[8] A range of defences apply, including where the person was exercising a power, or performing a function or duty, in the person's capacity as a Commonwealth officer or a person who is otherwise engaged to perform work for a Commonwealth entity.[9]

As secrecy provisions extend to Australian government agencies' handling of personal information, they overlap with certain provisions in the Privacy Act. For example, APP 12 outlines an APP entity's[10] obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies. To limit uncertainty regarding the intersection of obligations, I generally suggest that secrecy provisions that regulate personal information make clear their interaction with the Privacy Act.

In the Espionage and Other Offences Bill, this could be clarified in the Bill or EM by explaining that the secrecy provisions are not intended to impact on:

- the right to request access to an individual's personal information under APP 12 of the Privacy Act, or to obtain access under the FOI Act[11]
- the requirement for regulated entities to disclose certain information about an eligible data breach in accordance with the NDB scheme, under Part IIIC of the Privacy Act.

The NDB scheme applies to all agencies and organisations with existing personal information security obligations under the Privacy Act from 22 February 2018. It introduces an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm, as well as notifying me, as Australian Information Commissioner. Exceptions to notifying individuals or the Commissioner, may apply where a Commonwealth law prohibits or regulates the use or disclosure of information (a secrecy provision).[12] In particular:

---

[7] Para 95, EM to the Espionage and Other Offences Bill.

[8] Inherently harmful information is defined in section 121.1 of the Espionage and Other Offences Bill.

[9] Section 122.5 of the Espionage and Other Offences Bill.

[10] APP entity, as defined in section 6(1) of the Privacy Act, means an 'agency or organisation'. The terms 'agency' and 'organisation' are defined in section 6(1) of the Privacy Act and section 6C of the Privacy Act respectively.

[11] See section 38(2) of the FOI Act

[12] See sections 26WP(2) and 26WP(3) of the *Privacy Amendment (Notifiable Data Breaches) Act 2017.*

- the requirement to provide a statement to the Commissioner about the eligible data breach does not apply to the extent that this requirement is inconsistent with a secrecy provision (s 26WP(2))
- the requirement to notify individuals about an eligible data breach does not apply to the extent that providing this notice is inconsistent with a secrecy provision (s 26WP(3)).

My Office's relevant NDB advisory guidance notes that 'if a secrecy provision permits the disclosure of information in the course of an officer's duties, there would not be inconsistency between the secrecy provision and the NDB scheme notification requirements, as complying with the notification requirements is the responsibility of the agency through its officers.'[13] While it would appear that the defence in section 122.5 of the Espionage and Other Offences Bill would therefore permit disclosures under the NDB Scheme, clarification would be useful to limit any uncertainty. I suggest clarification could be provided by inserting a note into the Bill or including additional information in the EM to the Bill.

Foreign Influence Transparency Scheme Bill 2017

The Foreign Influence Bill would establish the Foreign Influence Transparency Scheme (the Scheme). Under the Scheme, a person will be required to apply for registration in certain circumstances,[14] and to report further information to the Secretary when various circumstances arise.[15] I understand that the Foreign Influence Bill requires the Secretary to maintain a register of this and other information,[16] and to publish certain information, including personal information, on a website.[17] The Secretary would also have the power to compel a person to provide information,[18] and to communicate scheme information to specified persons.[19]

As noted in the EM, the provisions of the Bill place some limitations on the right to privacy.[20] Given the collection, use and disclosure of personal information that would be authorised by the Bill, I suggest that the Attorney-General's Department consider conducting a PIA to identify the impact that the Scheme might have on the privacy of individuals. A PIA is a systematic assessment of a project (including, for example, new legislation) that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. Completing a PIA may assist the Department in clarifying the personal information that may be affected by the draft Bill's provisions, and help to mitigate any ensuing privacy risks.

---

[13] See OAIC guidance, *Exceptions to Notification Obligations*, <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/exceptions-to-notification-obligations>.

[14] Section 16.

[15] Part 3.

[16] Section 42.

[17] Section 43.

[18] Sections 45 and 46.

[19] Section 53.

[20] Explanatory Memorandum, pp 13–14.

My Office has published a Guide to undertaking PIAs, which may be helpful in this regard, as well as a PIA e-learning tool.[21] I also note that when the OAIC's *Privacy (Australia Government Agencies—Governance) APP Code 2017* enters into force from July 2018, Australian government agencies will be required to undertake a PIA in some circumstances.[22]

Additionally, I note that a number of the powers and requirements under the Foreign Influence Bill appear to be discretionary[23] or will depend on additional information set out in rules.[24]

Where discretionary powers or rules could authorise collections, uses or disclosures of personal information that have an impact on individuals' privacy, the mechanism for future authorisations or requirements may more appropriately occur through primary legislation. Alternatively, it may be appropriate to include obligations in the primary legislation to ensure that privacy is given appropriate consideration in the development of those rules.

I note, for example, that the rule making power under s 53 of the Foreign Influence Bill includes a requirement, under s 53(2), for the Minister to consult the Information Commissioner before making rules that would authorise the Secretary to communicate scheme information to prescribed persons for prescribed purposes. I suggest a similar requirement should be included for other discretionary powers or rules that could have an impact on individuals' privacy.

If you wish to discuss any of these matters further, please contact Sophie Higgins, Director, Regulation and Strategy, [redacted]

Yours sincerely

Timothy Pilgrim PSM
Australian Information Commissioner
Australian Privacy Commissioner

23 January 2018

---

[21] Available at <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments> and <https://www.oaic.gov.au/elearning/pia/welcome.html>.

[22] For more information on the *Privacy (Australia Government Agencies—Governance) APP Code 2017*, see <https://www.oaic.gov.au/privacy-law/australian-government-agencies-privacy-code>.

[23] For example, s 16(2)(d) and 42(2)(g).

[24] For example, s 43(1)(c).