



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: D2017/004501

Senator the Hon. Ian Macdonald
Chair, Senate Legal and Constitutional Affairs Legislation Committee
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Senator

Submission to the Inquiry into the Crimes Legislation Amendment (Powers, Offences and Other Measures) Bill 2017

I welcome the opportunity to comment on the provisions of the *Crimes Legislation Amendment (Powers, Offences and Other Measures) Bill 2017* (the Bill), as part of the Inquiry by the Senate Legal and Constitutional Affairs Legislation Committee (the Committee). I have focussed my comments on the provisions of Schedules 1 and 7 to the Bill, which seek to expand the circumstances in which personal information may lawfully be collected, used or disclosed and may therefore have an impact on the privacy of individuals.

By way of overall comment, I am supportive of measures which aim to address fraud and corruption, and enable law enforcement bodies to effectively cooperate and provide assistance to international organisations. The right to privacy is not absolute and in some circumstances, privacy rights must necessarily give way where there is a compelling public interest reason to do so. However, proposals which require or authorise the collection, use or disclosure of personal information should aim to strike an appropriate balance, and be reasonable, necessary and proportionate, having regard to the objectives they seek to achieve. Agencies should also ensure transparency in relation to their information-sharing practices, so that individuals know how their personal information will be handled.

Privacy impacts of the Bill

Schedule 1 – Functions of the Australian Federal Police – assistance and sharing information

The provisions of Schedule 1 to the Bill seek to make amendments to the *Australian Federal Police Act 1979* (Cth) (AFP Act) to enable the Australian Federal Police (AFP) to provide assistance and cooperation to international organisations and non-government organisations in relation to the provision of police services or police support services. The Bill does this by providing that the functions of the AFP encompass 'cooperation' with international organisations and non-government organisations (in relation to acts, omissions, matters or

things outside Australia, in relation to the provision of police services or police support services).

As discussed further below, I note that on the face of the Bill, it is not apparent:

- how the provisions will authorise the sharing of personal information
- the specific information to which they relate, or
- the non-government organisations the provisions are intended to capture.

I would therefore suggest that the Committee consider whether the Bill has been drafted as clearly and as narrowly as possible, and that any authorisations for the collection, use or disclosure of personal information are clearly set out in the legislation or where appropriate, explained in the Explanatory Memorandum (EM) to the Bill.

I would also recommend that the Attorney-General's Department (AGD) undertake a Privacy Impact Assessment (PIA) on the Schedule 1 provisions, paying particular attention to the matters identified below, if it has not done so already.¹ Conducting a PIA would assist in identifying any privacy impacts associated with the handling of the relevant personal information, and provide an opportunity to take proactive steps to mitigate any impacts.

Authorisation of information sharing

The EM to the Bill states that Schedule 1 allows for the sharing of information between the AFP and a range of international bodies such as Interpol, United Nations organisations, and non-government organisations. It appears from the EM that the intention of this measure is to invoke the exceptions in the Australian Privacy Principles (APPs) to broaden information sharing arrangements.

In particular, APP 6.2 (b) contains an exception to the general requirement that an agency must not use or disclose 'personal information' for a secondary purpose, if the use or disclosure of information is 'required or authorised by or under an Australian law'. However, a law will not authorise an exception to these requirements unless it does so by clear and direct language. In addition, an act or practice will not be authorised solely because an agency has a general (or incidental) statutory power to carry out its prescribed functions.²

While the Bill makes amendments to the functions of the AFP to encompass 'cooperation' and 'assistance' with international organisations and non-government organisations, the provisions do not explicitly authorise or refer to information sharing practices with such bodies. It is therefore unclear whether the provisions of the Bill are drafted clearly enough to invoke the APP 6.2 (b) exception.

¹ A PIA is a written assessment which may assist in identifying the privacy impacts of the Bill, and provides an opportunity to set out any recommendations for managing, minimising or eliminating those impacts. For further information on undertaking a PIA please see the OAIC's Guide to undertaking a privacy impact assessment available at www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-undertaking-privacy-impact-assessments.

² This may be so even where that power may authorise the entity to do anything necessary or convenient for, or incidental to or consequential upon, the specific functions and powers of the agency. See the OAIC APP Guidelines – Chapter B: Key Concepts available at www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts.

As a result, it is difficult to discern what privacy impacts Schedule 1 to the Bill may have, and whether these impacts would be reasonable, necessary and proportionate to achieve the policy objective. It is also not clear what kinds of personal information would be collected, used or disclosed under the proposal.

Greater certainty and transparency about the privacy impacts could be achieved through clear, specific and direct language concerning the authorisation of information sharing practices. I therefore suggest that any authorisation for the collection, use or disclosure of personal information is clarified within the legislation (or in the EM, where appropriate).

Non-government organisations

The inclusion of cooperation with 'non-government organisations' within the functions of the AFP appears potentially broad, and, as such, could cover a wide range of bodies. There is no definition provided of 'non-government organisation', and it is therefore not clear which types of organisations this measure is intended to capture. By contrast, the Bill defines international organisations, and the EM further explains that this measure allows for information sharing with organisations such as the United Nations and its organs, Interpol, international judicial bodies, the International Committee of the Red Cross.

I suggest that the Committee consider whether this measure has been drafted as narrowly as possible, in order to permit disclosures to particular bodies where this would serve the specific, articulated policy objective of the Bill, or whether further specificity may be needed.

Cross-border disclosure of personal information

The EM to the Bill states that the use and disclosure of information will be subject to existing protections under the *Privacy Act 1988* (Cth) (Privacy Act). However, it is not clear from the provisions of the Bill whether APP 8.1, which outlines the steps an APP entity must take to protect personal information before it is disclosed overseas, will apply to the disclosure.

In particular, I note that an APP entity does not have to comply with APP 8.1 where the disclosure is 'required or authorised by or under an Australian law' (APP 8.2(c)). As outlined above, legislation will not invoke an 'authorised by law' exception unless it does so by clear and direct language. While it is not clear whether the intention of this measure is to invoke this exception, consideration should be given to whether the Bill is drafted as clearly and narrowly as practicable to ensure the appropriate handling of information when disclosed to bodies outside of Australia.

If the intention is to rely on the APP 8.2(c) exception, in addition to ensuring the provisions are drafted with sufficient clarity to enable this, I would suggest the Committee consider whether the establishment of administrative arrangements (such as memoranda of understanding or information-sharing protocols) with the relevant overseas recipients may be warranted. These could set out mutually agreed standards for the handling of personal information that provide protections comparable to the APPs, where possible.

Schedule 7 – Commonwealth fraud prevention and investigation arrangements

Schedule 7 to the Bill proposes to insert a new Part VIID in the *Crimes Act 1914* (Cth), which creates a scheme authorising the collection, use and disclosure of personal information by Commonwealth entities for the purposes of preventing, detecting, investigating or dealing with fraud or corruption against the Commonwealth. I understand these amendments aim to enable entities to gather the information they need to carry out their own internal fraud or corruption investigations, and therefore respond more effectively to these issues.

The Privacy Act provides a range of exceptions which enable the sharing of personal information in relation to suspected unlawful activity, serious misconduct, or law enforcement activities. For example, Item 2 of the table to s 16A of the Privacy Act provides that an agency can collect, use or disclose personal information as part of taking appropriate action in relation to suspected unlawful activity or serious misconduct (where this is related to that entity's own functions or activities). Further, APP 6.2(e) provides that personal information can be used or disclosed for a secondary purpose where an entity reasonably believes that the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

However, as the EM notes, at present these exceptions do not always apply in ways that enable the effective investigation of fraud and corruption against Commonwealth entities. This is primarily because Commonwealth agencies performing their own internal criminal investigation functions under the *Commonwealth Fraud Control Framework* may not be 'enforcement bodies' for the purposes of the Privacy Act.³ At present, agencies can take appropriate action in relation to allegations of fraud within their own agencies (relying on s 16A of the Privacy Act, for example). However, agencies may be unable to disclose personal information to non-law enforcement agencies investigating fraud (as this would not relate to their own functions or activities).

Schedule 7 will therefore have an impact on the privacy of individuals by authorising the disclosure of information in situations which would not currently be permitted. As outlined earlier, any law that invokes these exceptions should be drafted as narrowly as possible and be a reasonable, necessary and proportionate response to meeting the specific policy objectives of the Bill.

In this regard, I note that the AGD has undertaken a PIA⁴ in relation to Schedule 7 of the Bill. My Office has been consulted as part of that process, as well as during the policy development phase for the Schedule 7 measures. In line with the Office of the Australian Information Commissioner's *Guide to undertaking a Privacy Impact Assessment*, to enhance transparency I would encourage AGD to publish this PIA. I would also encourage AGD to continue to update the PIA to ensure an ongoing approach to managing privacy risks.

I also welcome the provisions of the Bill which enable the publication of guidelines as a privacy enhancing measure, to ensure the protection of individual privacy as part of the

³ The term 'enforcement body' is defined in section 6 of the *Privacy Act 1988*.


⁴ See footnote 1 above.

operation of these measures. The introduction of clear, rigorous and practical guidelines will assist agencies to understand their obligations under the Privacy Act. In particular, I would expect the guidelines to outline steps that should be taken to ensure a robust privacy management framework, and to seek to build in safeguards and embed a culture of privacy that enables compliance. The guidelines should also outline how agencies will ensure transparency in relation to the way that they collect, use and disclose their employees' personal information.

Given my proposed role in approving the guidelines, my Office would be pleased to be consulted during their development. I also note that my Office has a range of tools and resources that could usefully be built upon by AGD, to assist in providing tailored guidance to Commonwealth entities when implementing their new obligations under the Bill.⁵

If you wish to discuss any of these matters further, please contact Sarah Ghali, Director Regulation and Strategy, at _____ or _____.

Yours sincerely


Timothy Pilgrim PSM
Australian Information Commissioner
Australian Privacy Commissioner

23 June 2017

⁵ These include the *Privacy Management plan template* and *Privacy Management Framework: enabling compliance and encouraging good practice*, the *Guide to securing personal information*, the *Guide to undertaking privacy impact assessments* and the *Data breach notification — A guide to handling personal information security breaches*. These are available on www.oaic.gov.au/agencies-and-organisations/guides.