Australian Government
Office of the Australian Information Commissioner

Our reference: D2016/000916

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Committee Chair

Australian Crime Commission Amendment (National Policing Information) Bill 2015

I thank the Senate Legal and Constitutional Affairs Legislation Committee (the Committee) for the opportunity to comment on the *Australian Crime Commission Amendment (National Policing Information) Bill 2015* (the Bill). My comments are focused on those provisions of the Bill which relate to the handling of 'national policing information', which is information currently handled by CrimTrac.

In making the following comments, I recognise the importance of ensuring that national law enforcement information and intelligence capabilities are used as effectively as possible to support police to protect the community. However, this needs to be balanced with any impacts on individual privacy. This involves consideration of whether the Bill is a necessary and proportionate response to meeting a specific need of Australian government agencies.

Privacy impacts of the Bill

The Bill seeks to merge CrimTrac into the Australian Crime Commission (ACC), to allow these two agencies to share their criminal intelligence and information capabilities. The merger is intended to facilitate the adoption of a more effective, efficient and evidence-based response to crime by police, justice agencies and policy makers.[1]

As part of the merger, the Bill will create a new regime for the collection, use and disclosure of 'national policing information'. National policing information is intended to capture all information which is currently handled by CrimTrac. Information currently handled by CrimTrac includes a wide range of information obtained from police and other sources, and may include personal and sensitive information such as information about missing persons, individuals' criminal records, the DNA profiles of offenders, as well as of victims and volunteers, and fingerprint and palm images (as collected by police, and used for a range of verification, forensic and missing person location purposes). Further, the Bill gives the ACC's CEO and Board administrative powers to determine how this regime will operate.

[1] See p 2 of the Explanatory Memorandum to the Bill.

Under s 7 of the *Privacy Act 1988* (Cth) (Privacy Act), the ACC is not required to comply with the obligations in the Privacy Act, including the Australian Privacy Principles (APPs), unlike CrimTrac (whose activities are covered by the Privacy Act). Therefore, if this Bill is enacted as drafted, I understand that:

- the information currently held (and the functions currently exercised in relation to this information) by CrimTrac will no longer be subject to the protections in the Privacy Act, and
- the Australian Information Commissioner would no longer have oversight or enforcement powers in relation to that information or those functions.

For these reasons, the Bill has an impact on individual privacy.

As discussed further below, while some of these impacts may be able to be addressed using other, non-legislative means (for example, through the use of an information-handling protocol), I note that these would not be enforceable and may be subject to a change in policy in the future without Parliamentary oversight. Therefore, I consider that such an approach may not adequately address the potential privacy impacts of the Bill.

In respect of these potential impacts, I recommend that the Committee consider whether the obligations and oversight mechanisms in the Privacy Act could continue to apply to national policing information following CrimTrac's merger with the ACC.

Independent Oversight

As I understand it, a level of oversight for the handling of national policing information will remain in place, provided by the Commonwealth Ombudsman, the Australian Commission for Law Enforcement Integrity (ACLEI) and the Parliamentary Joint Committee on Law Enforcement. However, I note that the scope of that oversight differs from that currently provided by the Australian Information Commissioner (Information Commissioner) through the Office of the Australian Information Commissioner (OAIC).

The Privacy Act confers a range of privacy regulatory powers on the Information Commissioner. These include powers that allow my office to work with entities to facilitate legal compliance and best privacy practice, as well as investigative and enforcement powers to use in cases where a privacy breach has occurred.

As part of this, I have the power to conduct assessments of an APP entity's privacy practices.[2] An assessment provides an independent and systematic appraisal of how well an agency or organisation (or discrete part of an agency/organisation) complies with all or part of its privacy obligations. My office approaches assessments as an educative process, and compliance with the Privacy Act is seen as part of good management practice. I also have the power to require an agency to undertake a Privacy Impact Assessment (PIA) in certain circumstances.

[2] See Part IV of the Privacy Act.

In addition, I also have the power to investigate (and otherwise deal with) alleged interferences with privacy by entities covered by the Privacy Act (such as CrimTrac), as well as the power to investigate acts or practices of potential privacy breaches on my own initiative. In particular, the OAIC provides a free complaint conciliation service to individuals who consider that their privacy has been breached. While the Commonwealth Ombudsman also handles individual complaints, its remedial powers differ from those available to the Information Commissioner under the Privacy Act, which include powers to:

- make court-enforceable determinations
- award compensation and other remedies
- seek court-enforceable undertakings, and
- apply for civil penalty orders, where appropriate.[3]

If the Bill is passed in its current form, these oversight and regulatory activities would cease.

Obligations regarding quality, security, access and correction in relation to national policing information (Australian Privacy Principles 10, 11, 12 and 13)

I acknowledge that if the Bill is enacted, it may be possible for the ACC to use other non-legislative means, such as certain technical and administrative arrangements, to help to protect the quality and security of the information currently held by CrimTrac. However, the ACC will not have obligations under APPs 10 and 11 to ensure the quality and security of the personal information currently held by CrimTrac (as CrimTrac currently has).

In relation to the obligations in APPs 12 and 13, I understand that individuals may still be able to access and/or correct their personal information, by applying to the relevant State or Territory (usually police) agency which is the source of the information held by the ACC (where privacy or other legislation, such as freedom of information laws, in the individual's particular jurisdiction permit this). However, I note that:

- not all State and Territory jurisdictions have privacy or other legislation which gives individuals equivalent rights and protections in respect of their personal information, compared with the Privacy Act or *Freedom of Information Act 1982* (FOI Act), and
- not all information currently held by CrimTrac is sourced from other agencies.

In any event, the ACC will not be obliged, under APPs 12 and 13, to provide access to, or correct, any personal information which it holds, and for which it is the sole holder (as CrimTrac is currently required to do by virtue of its APP obligations). Individuals may, however, still be able to apply to the ACC to access and correct their personal information under the FOI Act in certain circumstances.

Application of the Privacy (Persons Reported as Missing) Rule 2014

Section 16A of the Privacy Act sets out when the existence of a 'permitted general situation' (PGS) will provide an exception to the general prohibition against an APP entity collecting personal or sensitive information about an individual without that individual's consent, or where that information may have been collected with consent (but the information is to be

[3] See, eg, Parts IV, V, VI and VIB of the Privacy Act.

used for a secondary or different purpose than that for which it was originally collected). One such PGS relates to a situation where personal information is sought about an individual, for the purposes of assisting an APP entity, body or person to locate a person who has been reported as missing.[4]

The *Privacy (Persons Reported as Missing) Rule 2014* governs the application of the missing person PGS, and currently applies to CrimTrac when it is handling personal information in relation to locating a person reported as missing.[5] The Rule acknowledges that a person reported as missing may have exercised their free choice to disassociate themselves from friends and family for legitimate reasons, including removing themselves from harmful environments. The Rule therefore requires CrimTrac to, among other things, respect any known wishes of a missing person when using or disclosing information about them. Examples of when an APP entity may be aware of an individual's wishes will depend on the circumstances, but will include where the individual has specifically requested that the APP entity does not use or disclose their personal information.

If the Bill is enacted, the *Privacy (Persons Reported as Missing) Rule 2014* would no longer apply to the personal information currently held by CrimTrac (ie national policing information), and the ACC would not be obliged by the Rule to respect any known wishes of persons reported as missing when using or disclosing information about them.

Recommendation 1 – consider whether the obligations in the Privacy Act could continue to apply to national policing information

I acknowledge that the new arrangements do build in some measures for the protection of information currently held by CrimTrac, for example in the form of strengthened non-disclosure provisions, and certain oversight mechanisms which may be introduced by the ACC Board.[6] However, on the basis of the current the Bill, and the explanation given in the Explanatory Memorandum, I do not consider that these measures will provide protections equivalent to those contained in the APPs.

I consider that the Privacy Act and APPs have, to date, set an appropriate standard for the handling of the personal information and sensitive information handled by CrimTrac. It is not apparent to me why it is necessary to remove the information currently held by CrimTrac from the protections, oversight and enforcement arrangements in the Privacy Act. I note that a similar view was also expressed by the Scrutiny of Bills Committee in relation to the recent *Australian Crime Commission Amendment (Criminology Research) Bill* (which had a similar effect in relation to research information formerly handled by the Australian Institute of Criminology, which was also merged with the ACC).[7]

Given the volume and sensitivity of the information currently held by CrimTrac, I am of the view that there would need to be cogent reasons for exempting that information, and the

---

[4] See s 16A of the Privacy Act, Item 3.
[5] See APP 6.2(c), and s 16A, Item 3.
[6] See the Explanatory Memorandum to the Bill.
[7] See the Senate Standing Committee for the Scrutiny of Bills: Alert Digest No. 12 of 2015 (11 November 2015), at p 2.

activities associated with it, from the Privacy Act entirely. I consider that the objectives of the regime could be met, while at the same time retaining the protections and oversight offered by the Privacy Act.

In light of this, I recommend that the Committee consider whether the new national policing information functions of the ACC could be carried out without exempting those functions from the Privacy Act.

The Statement of Compatibility with Human Rights

The approach I have outlined above to assessing the privacy impacts of this Bill is consistent with that taken in applying the right to privacy in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), to which the Privacy Act, in part, gives effect. In line with Article 17 of the ICCPR, the Privacy Act recognises that the protection of individuals' privacy, through the protection of their personal information, cannot be an absolute right. Rather, those interests must be balanced with the broader interest of the community in ensuring that entities are able to carry out their legitimate functions and activities. However, where handling of individuals' personal information is authorised in the broader interests of the community, any such limitation on the privacy protections should be reasonable, proportional and necessary for the policy objective.

While the Statement included in the Explanatory Memorandum acknowledges that this Bill engages the right to privacy, it does not make all of the privacy impacts of this Bill explicit (and in particular, that by merging the two agencies, the Bill removes national policing information from the coverage of the Privacy Act). I suggest that consideration be given to further explaining in the Statement how the provisions of the Bill are compatible with Article 17 of the ICCPR, and in particular, how the specific privacy impacts will be addressed.

Recommendation 2 – Publication of the PIA in relation to the Bill

I am pleased that the Attorney-General's Department (AGD) has undertaken a PIA[8] in relation to the Bill, and that my office has been consulted as part of that process.

As with all PIAs, and in line with the OAIC's *Guide to undertaking a Privacy Impact Assessment*, I encourage AGD to publish this PIA (to the extent that this is appropriate, and would not reveal any sensitive intelligence or policing information). In this particular case, publication of the PIA may assist in promoting transparency around the protections that will be afforded to the information currently held by CrimTrac, should the Bill be enacted.

[8] 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*.

Should the Committee require any further information please contact , Director, Regulation and Strategy Branch, on or via email on

Yours sincerely

Timothy Pilgrim PSM
Acting Australian Information Commissioner

18 February 2016