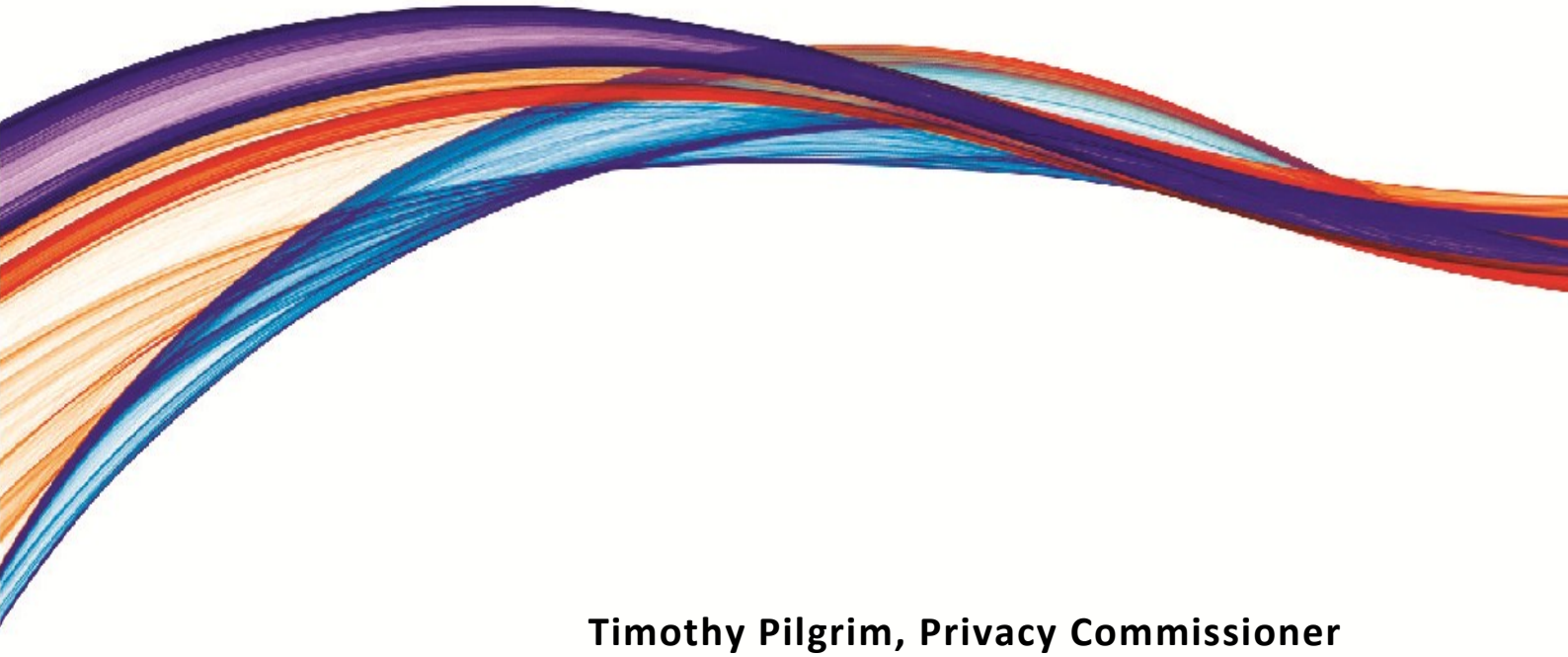
Australian Government

Office of the Australian Information Commissioner

National Gambling Reform Bill 2012

Submission to the Joint Select Committee on Gambling Reform

13 November 2012



Timothy Pilgrim, Privacy Commissioner

Executive Summary

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide comment to the Joint Select Committee on Gambling Reform about the National Gambling Reform Bill 2012 (the Bill).[1]

The OAIC understands the object of the Bill is to reduce the harm caused by gaming machines to problem gamblers, their families and communities, and those at risk of experiencing that harm.[2] The Bill provides for precommitment systems for gaming machines, and for gaming machine users to register with a precommitment system.

The sensitive nature of the personal information that will be handled under the Bill means that serious consequences may arise for gaming machine users registered with a precommitment system if their personal information is not handled appropriately.

The OAIC welcomes arrangements in the Bill to support the privacy of registered users. However, the OAIC believes consideration should be given to how the Privacy Act will apply to personal information being handled under the Bill and the effectiveness of the privacy safeguards in the Bill.

Key recommendations

1. Privacy Impact Assessment (PIA) — The OAIC recommends the Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA) conduct a PIA. A PIA will assist in identifying the information flows within the system, and where additional privacy protections may be required. The OAIC notes a number of potential gaps in the regulation of personal information within the system and recommends consideration be given to:
    a. clarifying an individual's right to complain to the Australian Information Commissioner about an unauthorised use or disclosure of protected information that is also the individual's personal information
    b. bringing small business operators that are exempt from the Privacy Act, within the Privacy Act's coverage in relation to their handling of personal information under the Bill
    c. the regulation of personal information held under the Bill by state-based agencies and public bodies that are not subject to local binding privacy laws
    d. reducing the fragmentation of oversight mechanisms between multiple regulators under the Bill.

[1] http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=gamblingreform_ctte/gambling_reform_legislation_2012/index.htm

[2] Page 1 of the Explanatory Memorandum to the Bill.

2. Regulation-making powers — The OAIC recommends FaHCSIA consult widely with relevant agencies, entities and stakeholders before making regulations under the Bill.
3. Exchange of personal information between precommitment systems, registered users and gaming machines — The OAIC recommends that:
    a. precommitment systems should be designed to collect the minimum amount of personal information necessary to achieve the system's purposes, and in a way that is sensitive to the privacy of the individual
    b. consideration be given to designing and approving precommitment systems in a way that ensures that communications between precommitment systems, registered users and gaming machines are made in a manner that maintains the privacy of the information.
4. Retention periods for personal information collected by the Regulator — The OAIC recommends consideration be given to including a requirement in the Bill for the Regulator to destroy or permanently de-identify protected information on the basis the Regulator no longer needs the protected information for any purpose under the Bill except where the information is contained in a Commonwealth record (as defined in the *Archives Act 1983*), or the Regulator is required by or under an Australian law to retain the information.
5. Use of the term 'biometric processes' —The OAIC recommends that for clarity and consistency, terms regarding the use of biometric information in the Bill should be consistent with those in the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (the Privacy Amendment Bill).
6. Penalties for establishing a national database — The OAIC recommends consideration should be given to including a penalty provision for establishing a national database of protected information that has been obtained from precommitment systems.
7. Disclosure of summaries or statistics — The OAIC recommends disclosure by the Regulator for the purposes of summaries or statistics should only be permitted where the information is permanently de-identified.
8. Disclosure of protected information to the Minister — The OAIC recommends consideration be given to limiting the Regulator's power to disclose protected information to the Minister for 'purposes under the Act'.

The Office of the Australian Information Commissioner

The OAIC was established by the *Australian Information Commissioner Act 2010* (the AIC Act) and commenced operation on 1 November 2010.

The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner.

The former Office of the Privacy Commissioner was integrated into the OAIC on 1 November 2010.

The OAIC brings together the functions of information policy and independent oversight of privacy protection and freedom of information (FOI) in one agency, to advance the development of consistent workable information policy across all Australian government agencies.

The Commissioners of the OAIC share two broad functions:

- the FOI functions, set out in s 8 of the AIC Act — providing access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982*, and
- the privacy functions, set out in s 9 of the AIC Act — protecting the privacy of individuals in accordance with the *Privacy Act 1988* (the Privacy Act) and other legislation.

The Information Commissioner also has the information commissioner functions, set out in s 7 of the AIC Act. Those comprise strategic functions relating to information management by the Australian Government.

Introduction

Overview of the National Gambling Reform Bill 2012

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide comment to the Joint Select Committee on Gambling Reform about the National Gambling Reform Bill 2012 (the Bill).[3]

The OAIC understands the object of the Bill is to reduce the harm caused by gaming machines to problem gamblers, their families and communities, and those at risk of experiencing that harm.[4]

The Bill proposes to introduce a number of harm minimisation measures in relation to gambling on gaming machines. The Bill requires:

- new gaming machines manufactured or imported from the end of 2013 to be capable of supporting precommitment[5]
- each state or territory to allow a gaming machine user to register to use a precommitment system and set a limit on the amount that he or she is prepared to lose during a given period using gaming machines located in that State or Territory[6]

[3] http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=gamblingreform_ctte/gambling_reform_legislation_2012/index.htm
[4] Page 1 of the Explanatory Memorandum to the Bill.
[5] Clause 15 of the Bill.
[6] Clauses 19, 21 and 22 of the Bill.

- all gaming machines to display dynamic warnings about the harm from and the cost of using gaming machines — the warnings may be general or relate to a specific person[7]

- limitations on withdrawals from automatic teller machines located in gaming premises (excluding casinos).[8]

In addition, the Bill establishes a Regulator,[9] a penalty regime, and a monitoring and enforcement regime.[10]

The OAIC, in particular, welcomes arrangements in the Bill to support the privacy of registered gaming machine users (registered users).[11]

Privacy regulation and the Bill

The Privacy Act regulates the handling of personal information by Australian, ACT and Norfolk Island Government agencies, and private-sector organisations, including the collection, use, disclosure, security, access to and correction of that information.[12] An act or practice by an agency or organisation that breaches the Privacy Act is an interference with the privacy of the individual to whom the relevant personal information relates.[13] An individual may complain to the Australian Information Commissioner about an interference with their privacy.[14]

The Bill also provides additional privacy protections for certain types of personal information – referred to in the Bill as 'protected information'.[15]

The Bill defines protected information as information that relates to a person other than the person who obtains the information and is obtained by a person:[16]

- in the course of performing duties or functions, or exercising powers, under the Bill
- from the precommitment system, or
- by way of an authorised disclosure and is information to which one of the previous two criteria applied.

[7] Clause 38 of the Bill.
[8] Clause 39 of the Bill.
[9] Clause 104 of the Bill provides that the Regulator is the Secretary of the Department of the Minister who has portfolio responsibility for the new Act.
[10] Page 3 of the Explanatory Memorandum to the Bill.
[11] Chapter 4, Part 2 of the Bill.
[12] Section 6(1) of the Privacy Act defines 'personal information' as: '…information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.
[13] Division 1 of Part III of the Privacy Act.
[14] Section 36 of the Privacy Act.
[15] Clause 67(5) of the Bill.
[16] Clause 67(5) of the Bill.

The Bill sets out the circumstances where use or disclosure of protected information is authorised.[17] The Bill also provides for a number of offences for the unauthorised use or disclosure of protected information.[18] These offences are intended to apply in addition to remedies available under the Privacy Act.[19]

Comments on the National Gambling Reform Bill

Privacy Impact Assessment

A PIA is a tool designed to help identify and respond to the privacy ramifications of new or existing systems. A PIA will assist in identifying where there may be gaps in the regulation of personal information within the system, and where additional privacy protections may be required. Generally, a PIA should

- describe the personal information flows in a project
- analyse the possible privacy impacts of those flows
- assess the impact the project as a whole may have on the privacy of individuals
- explain how those impacts will be eliminated or minimised.

While the OAIC acknowledges arrangements in the Bill to support the privacy of registered users, the OAIC is concerned that there is a lack of clarity about information flows in the Bill, and the protections afforded to personal information by federal or state-based privacy regimes. There is a risk that the arrangements in the Bill and existing privacy protections in the Privacy Act will not cover all persons and entities involved in the precommitment system, or it may cover them in an inconsistent way. This may prevent registered users whose personal information has been mishandled from accessing an appropriate remedy under the Privacy Act, the Bill or other state-based privacy regime. Conducting a PIA will assist in identifying and addressing these gaps and inconsistencies.

The OAIC has published a guide outlining the steps agencies should take in conducting a PIA. A copy of the PIA Guide is available on the OAIC's website.[20]

Enhancing privacy protections

Remedies for individuals if there is an unauthorised use or disclosure of personal information

The OAIC is concerned to ensure that individuals are able to access a remedy in the event that there is an unauthorised use or disclosure of their personal information under the Bill.

[17] Clauses 68-77 of the Bill.
[18] Clause 67 of the Bill.
[19] Page 33 of the Explanatory Memorandum to the Bill.
[20] *Privacy Impact Assessment Guide*, 2010, http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.html

As mentioned above, the Bill provides for a number of offences for the unauthorised use or disclosure of protected information.[21] The OAIC acknowledges that the definition of 'protected information' is beyond the definition of 'personal information' contained in the Privacy Act.[22] However, it is unclear whether an individual is able to access a remedy if there is an unauthorised use or disclosure of protected information under the Bill, where that information is also the individual's personal information. For example, it is unclear whether an individual will be able to complain to the Australian Information Commissioner about the unauthorised use or disclosure of protected information under the Bill, where that information is also the individual's personal information.

The OAIC recommends that consideration be given to clarifying in the Bill an individual's right to complain to the Australian Information Commissioner about an unauthorised use or disclosure of protected information that is also the individual's personal information. For example, the Bill could include a provision[23] that makes an unauthorised use or disclosure of protected information under the Bill, where that information is also personal information (as defined in s 6 of the Privacy Act), an act or practice that is an interference with the privacy of the individual to whom the personal information relates, for the purposes of ss 13 or 13A of the Privacy Act.[24] A note to that provision could clarify that such acts or practices may be the subject of a complaint under s 36 of the Privacy Act. It may also be necessary to insert a note referring to that provision into ss 13 and 13A of the Privacy Act.

Small business operators

The OAIC understands that the Regulator will have the power to licence 'persons' to provide, operate, repair, maintain or install precommitment systems for gaming machines.[25] If a person is licenced, they may then apply for approval of the precommitment system for a state or territory.[26] The licensed person and any employees will likely have access to the personal information of registered users contained in the precommitment system.

The Bill regulates collection, disclosure and use of protected information, and to some extent a registered user's access to their protected information. In addition, the National Privacy Principles (NPPs) contained in the Privacy Act, regulate the handling of personal information by organisations, including the collection, use, disclosure, security, access and correction of that information.

[21] Clause 67 of the Bill.
[22] Page 33 of the Explanatory Memorandum to the Bill.
[23] The OAIC notes that the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 is currently before Parliament. Consideration may need to be given to that Bill when drafting any such provision.
[24] The OAIC notes that this is the approach adopted in various other pieces of legislation. See, for example, s 173 of the *Personal Property Securities Act 2009* and s 35L of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.
[25] Clause 56 of the Bill.
[26] Clause 46 of the Bill.

While all licensed persons and employees will need to comply with provisions in the Bill when handling protected information,[27] the OAIC is concerned that if 'small business operators' (SBOs) with an annual turnover of $3 million or less and who are exempt from the NPPs,[28] are licenced by the Regulator, then registered users may not have a remedy under the Privacy Act if their personal information is mishandled.[29] This inconsistency potentially creates a gap in the protection of the handling of personal information by licensed persons that are SBOs.

For example, NPP 6 generally requires an organisation that holds personal information about an individual to provide the individual with access to that information. Further, NPP 6 requires organisations to correct information that the individual establishes is not accurate, complete and up-to date. However, the Bill only requires a precommitment system to provide a person with their 'transaction statement'.[30] The 'transaction statement' is a written statement that contains certain personal information about the person. The Bill does not require a precommitment system to provide the individual with access to all personal information held about them by the precommitment system, or to correct that information.

The OAIC recommends consideration be given to addressing this potential gap in the regulation of personal information. For example, there is a provision in s 6E of the Privacy Act which extends the Privacy Act to cover small businesses in relation to their Anti-Money Laundering/Counter-Terrorism Financing compliance activities. A similar approach could be adopted for precommitment systems provided, operated or maintained by licensed persons that are SBOs.

State and territory privacy regimes

The OAIC is concerned that personal information handled by some state or territory agencies or public bodies under the Bill may not be covered by privacy laws.

The Bill gives the Regulator the power to delegate all or any powers or functions under the Bill (other than under cl 113) to a senior public servant of a state or territory or to a body established for a public purpose by or under a law of a state or territory, with the written agreement of the relevant state or territory Minister.[31] Also, the Regulator may make arrangements with an agency of a state or territory, for the services of officers or employees of the agency to be made available to assist the Regulator in performing her is her functions or duties, or exercising his or her powers.[32] This may mean that a state or territory agency or public body will be handling information under the Bill, which may include personal information of a sensitive nature.

[27] Clause 67(2) of the Bill.
[28] Sections 6C and 6D of the Privacy Act.
[29] Section 13 of the Privacy Act.
[30] Clause 34 of the Bill.
[31] Clause 200 of the Bill.
[32] Clause 108 of the Bill.

The Privacy Act does not generally apply to state or territory agencies or public bodies.[33] In circumstances where state agencies or public bodies are not subject to local binding privacy laws, there are potential gaps and inconsistencies in the protection afforded to personal information handled under the Bill.

The OAIC recommends consideration be given to the regulation of state-based agencies and public bodies operating outside of the jurisdiction of the Privacy Act or other local binding privacy laws, to ensure full protection of personal information that will be handled under the Bill.

Potential for fragmentation of oversight mechanisms

The OAIC is concerned that delegating the Regulator's powers or functions to state or territory agencies or public bodies, or allowing state or territory officers or employees to assist the Regulator (see 'State and territory privacy regimes' above) may result in the fragmentation of oversight mechanisms.

While the model chosen for this Bill may be affected by constitutional and policy constraints, the OAIC is concerned to ensure that consistent independent oversight mechanisms are in place, particularly in terms of privacy.

We note that oversight mechanisms performed by multiple regulators can lead to confusion about where to complain, differing legislative interpretations and complaints outcomes, and unnecessary duplication of effort and expenditure.

The OAIC recommends that consideration be given to reducing the fragmentation of these mechanisms.

Regulation-making powers

The OAIC notes a number of details regarding the operation of precommitment systems are to be dealt with by the regulations, rather than being detailed in the Bill.

Where regulation-making powers are to be used, the OAIC recommends FaHCSIA consult widely with relevant agencies, entities and stakeholders before making regulations.

Exchange of personal information between pre-commitment systems, registered users and gaming machines

Identification of registered users

The Bill does not contain specific provisions about what information will be collected when an individual registers with a pre-commitment system, and how registered users will identify themselves to gaming machines. These matters are left to the regulations,[34]

[33] Section 6(1) of the Privacy Act defines 'agency'. The Privacy Act does, however, apply in a slightly amended version to Australian Capital Territory government agencies under s 23 of the *Australian Capital Territory Government Service (Consequential Provisions) Act 1994*.

[34] Clause 23(3) and 29(4) of the Bill.

although the OAIC acknowledges the inclusion of clauses prohibiting the use of 'biometric processes' to identify a registered user.[35]

The OAIC recommends that precommitment systems should be designed to collect the minimum amount of personal information necessary to achieve the system's purposes, and in a way that is sensitive to the privacy of the individual. Conducting a PIA will assist in determining this. The OAIC would appreciate the opportunity to consider and comment on any draft regulations made for this purpose.

Information displayed by gaming machines in a public venue

The Bill requires gaming machines to display certain information about and to a registered user, including the registered user's loss limit, limit period and amount remaining of the loss limit for the current limit period.[36] Gaming machines are also required to display dynamic warnings that relate to the use by a specific person of the gaming machine, which may also include personal information.[37]

The OAIC notes that the information to be displayed by gaming machines includes personal information of a sensitive nature. Since registration for precommitment under the Bill is not mandatory,[38] the fact an individual has chosen to register may, for example, imply that the individual has a gambling problem. The fact that information is being displayed implies that the person using the gaming machine is a registered user. The information displayed also includes financial information.

The OAIC is concerned to ensure that this information is displayed in a way that is consistent with the private and sensitive nature of the information – for example, information displayed by a gaming machine may be viewable by other persons in the gaming venue. If the information is displayed in a way that is not consistent with the private and sensitive nature of the information, it may make individuals reluctant to register for precommitment.

The OAIC recommends that consideration be given to designing and approving precommitment systems in a way that ensures these communications are made in a manner that maintains the privacy of the information. Conducting a PIA may assist in addressing this issue.

Retention periods for personal information collected by the Regulator

The OAIC is concerned that the Bill does not specify the duration for which protected information collected by the Regulator from precommitment systems will be retained or when it will be de-identified. As the protected information being collected by the Regulator from precommitment systems includes personal information of a sensitive nature, the OAIC is mindful of reducing the risk of the information being mishandled. This

[35] Clauses 23(2) and 29(3) of the Bill.
[36] Clause 31 of the Bill.
[37] Clause 38 of the Bill.
[38] Clause 21 of the Bill.

can be ensured by permanently de-identifying or destroying the protected information once it is no longer needed for any purpose under the Bill.

The OAIC notes a precommitment system that is an organisation for the purposes of the Privacy Act will need to comply with NPP 4 regarding data security.[39] Under NPP 4.2, a precommitment system must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP 2.

In contrast, the Regulator, as an Australian Government agency, will be subject to the Information Privacy Principles (IPPs), which do not contain an equivalent provision regarding the destruction or de-identification of personal information. The OAIC notes that the Privacy Amendment Bill, which is currently before Parliament, would require the Regulator, to take such steps as are reasonable in the circumstances to destroy or de-identify the information if it is no longer needed for any purpose for which it may be used or disclosed under the Bill, except where the information is contained in a Commonwealth record (as defined in the *Archives Act 1983*), or the Regulator is required by or under an Australian law to retain the information.[40] However, until the Privacy Amendment Bill commences, the Regulator will continue to be bound by the IPPs.

The OAIC therefore recommends that consideration be given to including a requirement in the Bill for the Regulator to destroy or permanently de-identify protected information on the basis the Regulator no longer needs the protected information for any purpose under the Bill, except where the information is contained in a Commonwealth record (as defined in the *Archives Act 1983*), or the Regulator is required by or under an Australian law to retain the information.

Other matters

The OAIC notes a number of areas of the Bill where privacy protections could be enhanced.

Use of the term 'biometric processes'

The OAIC notes the inclusion of clauses prohibiting the use of 'biometric processes' to identify a person who chooses to register through a precommitment system or to identify whether the person is registered for a precommitment system in a State or Territory.[41] The OAIC understands the purpose of these clauses is to protect the privacy of registered users.[42]

[39] Section 6C of the Privacy Act defines organisation as: an individual, body corporate, partnership, any other unincorporated association or trust that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.
[40] Australian Privacy Principle 11.2(b) of the Privacy Amendment Bill.
[41] Clauses 23(2) and 29(3) of the Bill.
[42] Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 2012, 2 (Jenny Macklin).

The OAIC notes that the Privacy Amendment Bill uses the terms 'biometric information' and 'biometric templates' in relation to the definition of 'sensitive information'.[43]

The OAIC recommends that for clarity and consistency, consideration should be given to using terms consistent with those in the Privacy Amendment Bill.

Penalties for establishing a national database

The OAIC welcomes the requirement under the Bill that 'a national database of protected information that has been obtained from precommitment systems must not be established'.[44]

The OAIC understands the purpose of this clause is to protect the privacy of registered users.[45] However, there is no specific penalty for breaching this prohibition.

The OAIC recommends consideration should be given to including a penalty provision.

Summaries or statistics derived from protected information

Clause 77 of the Bill permits the Regulator to disclose summaries of protected information or statistics derived from protected information if those summaries or statistics are 'not likely to enable the identification of a person'.

As an increasing number of datasets are made available for purposes under the Bill, there is a risk that de-identified information could be linked back to the registered user. Reasonable, but thorough, steps should be taken by the Regulator to de-identify the data in a permanent way that prevents re-identification.

The OAIC recommends that disclosure for this purpose should only be permitted where the information is permanently de-identified.

Disclosure of protected information to the Minister

The OAIC believes that the authorisation to disclose protected information to the Minister may be unintentionally broad. The Bill allows the Regulator to disclose protected information to the Minister without any limitation.[46]

The Explanatory Memorandum to the Bill gives examples where protected information would be disclosed to the Minister. For example, information may be disclosed for the purpose of a meeting or forum that the Minister is to attend.[47]

The OAIC recommends that further consideration be given to limiting the Regulator's power to disclose protected information to the Minister for certain purposes, such as 'purposes under the Act', as is the case for disclosures to 'entrusted persons'.

[43] Clause 6(1) of the Privacy Amendment (Enhancing Privacy Protection) Bill 2012.
[44] Clause 36 of the Bill.
[45] Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 2012, 2 (Jenny Macklin).
[46] Clause 74 of the Bill.
[47] Page 38 of the Explanatory Memorandum to the Bill.