Office of the Information Commissioner
Queensland

Submission to the Finance and Public Administration Legislation Committee on the exposure draft of the Australian Privacy Amendment Legislation

(28 July 2010)

Office of the Information Commissioner (Qld)
PO Box 10143
Brisbane Adelaide St Qld 4000
(07) 3005 7155

The Queensland Office of the Information Commissioner is an independent statutory authority. This submission does not represent the views or opinions of the Queensland Government.

Thank you for the opportunity to make a submission to the Finance and Public Administration Legislation Committee (**the Committee**) on the exposure draft of the Australian Privacy Amendment Legislation.

The Office of the Information Commissioner Queensland (**OIC**) has, under the *Information Privacy Act 2009* (Qld), the capacity to provide public comment on any matter which relates to public sector privacy.

The OIC would be pleased to offer further assistance or expand on any of the points raised in this submission should it be requested.

APP 1 - obligation to comply

Australian Privacy Principle 1 (**APP 1**) requires an entity to take such steps as are reasonable in the circumstances to implement practices, procedures and systems which will ensure the entity complies with the Australian Privacy Principles (**APPs**). The OIC has concerns over the wording of APP 1. OIC recognises that principles-based legislation is the best way of addressing the need for privacy protection as this approach allows for a flexible and adaptable model of regulation. However, OIC does not believe that the obligation to comply with those principles should necessarily carry the same flexibility.

It is consistent across the Australian jurisdictions which have enacted information privacy laws that while they contain privacy principles similar to the APPs, the obligation to comply with the principles is mandatory and not subject to a 'reasonable in the circumstances' test. OIC considers the adaptable and flexible nature of the APPs provides sufficient scope for entities to implement them in ways which are reasonable, based on the circumstances and context of the entity's personal information handling.

The OIC recommends the Committee consider APP 1 in terms of whether or not it would be more appropriately stated as a mandatory obligation rather than subject to a 'reasonable in the circumstances' test.

APP 3 - collection – where necessary for, or related to, an entity's functions or activities

APP 3 regulates the collection of personal information by an entity, including personal information which is sensitive information. It provides that an entity must not collect personal information unless it is:

- reasonably necessary for one or more of the entity's functions or activities, or
- directly related to one or more the entity's functions or activities.

The OIC has a concern over the way APP 3 is worded, as it appears to create a situation where an entity could collect personal information that it did not need, so long as it could establish a direct relationship between the information and its functions or activities. An example would be a broad category such as crime prevention – it would not be difficult for an entity to argue that collecting any personal information of the Australian community could not be in some way related to this category.

The OIC recommends that the Committee consider whether this is an intended outcome of APP 3 and whether it would be more appropriate to limit the otherwise wide meaning of 'directly related to its functions or activities' by including words that require the entity to demonstrate an immediate need for that information in order to carry out its functions or activities or, alternatively, to change the 'or' to an 'and', which would limit collection of personal information to that which was reasonably necessary for an entity's functions or activities.

Necessary to lessen or prevent a serious threat

A number of the APPs create a general rule and then provide exceptions to it. One of the exceptions which recurs in a number of APPs is:

> [T]*he entity reasonably believes that the* [action] *is necessary to prevent a serious threat to the life, health or safety of any individual, or to public health or safety.*

The *Information Privacy Act 2009* (Qld) contains a similar exception in its privacy principles relating to use and disclosure; however the 'welfare of an individual' and 'the welfare of the public' are included with the categories of life, health and safety.

The OIC would recommend the Committee consider whether it would be appropriate to broaden this exception everywhere it appears in the APPs to include individual or public welfare'. This would provide a greater scope for the remedying of serious situations which might not fall within the life, health and safety categories. For example, an outbreak of disease that threatens crops or livestock may require the sharing of personal information, such as the identities of owners of vehicles which have been observed transporting the crops or livestock, between agencies across Australia in order contain it; it is unlikely that preventing a threat such as this would fall into the life, health or safety categories.

APPs 4 and 5 – dealing with unsolicited personal information

APP 4 requires an entity to consider, as far as is practicable, any unsolicited personal information it receives in light of the limitations in APP 3. APP 4(3) states that if, after having done so, an entity determines that APP 3 *would have* permitted the entity to collect the personal information, APPs 5 through 13 apply to that information.

APP 5 outlines the obligation to inform the individual the subject of the personal information of the matters listed in APP 5(2), so where unsolicited personal information *could have been* solicited by the entity under APP 3, the entity must meet the same obligations as *if it had* solicited it. OIC suggests that practically, this requirement imposes an immense administrative burden on entities. OIC notes that agencies are often the recipients of significant amounts of unsolicited personal information. OIC acknowledges that the obligation in APP 5 is predicated on the basis that the entity need only do what is reasonable in the circumstances.

Personal information provided by third parties

OIC notes that this obligation also applies to unsolicited information provided by third parties. OIC acknowledges that while in principle and in many practical circumstances it is of benefit to an individual to be informed that an entity holds personal information concerning them regardless of the source of that information. However, the requirement to notify the individual that the information has been provided by a third party does raise practical difficulties.

When an entity solicits information from an individual it does so either through a form or through direct contact with the individual. For both of these methods complying with collection obligations is a relatively simple and straightforward process – for example, the provision of the required information through a notice on the form.

However, when an entity sources personal information through a third party, it can do so in a myriad of ways and in circumstances where disclosure of the circumstances is either impractical and/or not desirable. One example is in the area of complaints and grievances where complainants and persons associated with the complaint may provide a great deal of personal information about a person who is the subject of the complaint. Notwithstanding obligations under natural justice/procedural fairness, there are matters of confidence in the management of the complaints which in some circumstances, create compelling reasons for identity of the complainant (at the least) to not be disclosed to the person who is the subject of the complaint.

In the above example, sub-section (f) also obligates the entity to inform the complainant, ideally at the time of making the complaint, that their personal information may be passed onto the person they are complaining about. This removes any element of confidentiality in a complaint process, which in many circumstances may deter complainants.

Difficulties would also arise when personal information is routinely and legitimately passed between entities. APP 5 would add a layer of administrative routine to an entity's processes. To give a Queensland example, vehicle registration and driver licence information, including contact details for owners and drivers are held by the Queensland Department of Transport and Main Roads. When the Queensland Police Service is dealing with traffic infringements, they routinely access the Department's data in order to prosecute the offence. APP5 would on its face, require that access to be disclosed to the individual concerned.

For this reason Queensland's privacy legislation requires notification of collection only when the information is collected from the individual concerned.

OIC further acknowledges that in the health area, APP 5 is both desirable and routine. However, in the areas other than health, the prevailing process has been to inform individuals of the circumstances of the collection only when the information is obtained directly from the individual concerned.

OIC submits that there are practical and sensible reasons for maintaining this distinction.

APP 4(4) goes on to state that, if the entity decides that APP 3 would *not have permitted* it to collect the personal information, the entity must either destroy or deidentify the personal information, but only where it is practicable, lawful and reasonable to do.

It is common for a person to provide their personal information to one entity either on a mistaken belief or through lack of knowledge, that the entity is responsible for dealing with the subject matter. In actuality, the subject matter is dealt with by another distinct entity. For example, a person may write to their relevant Police Service querying the conditions of trading licence which does not in itself raise an issue of criminality.

OIC recommends that the Committee consider adding words to APP 4 that clearly require personal information which is not destroyed or de-identified under APP 4(4) to be managed in accordance with APPs 6 through 13. OIC has no concerns with APP 5 not applying to this category of personal information.

OIC also recommends including an example after APP 4(4) which demonstrates when it

would be unlawful to destroy the personal information, and which includes a reference to the recordkeeping obligations of agencies.

In the alternative, it is arguable that the individual concerned intended the personal information to reach the entity that had the appropriate authority and permissions to deal with the subject matter and that accordingly, there is an implied consent for the disclosure of the material to that entity.

Rather than destroy or de-identify the information, there may be occasions where it is more expedient and of value to the person involved if the first entity could simply pass on the information to the appropriate entity. To cover this eventuality, a form of wording such as the following could be added:

If the entity determines that the entity could not have collected the personal information but is able to determine that another entity could have collected the personal information, the first entity can, as soon as practicable and only if it is lawful and reasonable to do so:

a) pass the information onto the appropriate entity; and

b) inform the individual about the passage

APP 6 – use or disclosure of personal information

APP6 permits the 'secondary'' use or disclosure of personal information if the information is not sensitive information and it is related to a 'primary' use or disclosure.

OIC respectfully suggests that the above test is so loose as to render the prohibition on secondary use or disclosure meaningless. Entities have specific areas of operation which are necessarily both broad albeit concentrated in a specific area. To provide a Queensland example, the purpose of Queensland's Department of Education and Training is "to engage Queenslanders in lifelong learning through education and training to enrich their lives."[1]

All activities conducted in an entity can be related to all other activities. For example, the entity's management of personnel is related to the achievements of that entity. Yet it could not be easily argued that the personal information of staff is in the same category as the personal information of the entity's 'clients'. Under APP6 the potential exists for the secondary use or disclosure of any personal information which in the control or possession of an entity irrespective that the primary purpose is widely different.

OIC acknowledges that the agency's capacity to use personal information for a secondary purpose is limted by the expectations of the individual concerned. However, this pre-disposes that the individual will have an informed knowledge of the business activities of the entity. It could also lead to the situation bloody-minded individual could dispute a secondary sue by simply stating 'I had no expectation that when I informed one area of the entity about my change of contact details, that this information would be passed onto other areas of the entity.'

In Queensland's privacy legislation the secondary purpose applies to use only and in addition, the test is that of 'direct relation' . Finally, the directly-related purpose is determined objectively rather than subjectively. OIC submits that provides a balance between practicality and protection and suggests the Committee similarly consider limiting the breadth of this permission.

APP 10 and 13 – accurate, up-to-date and complete

1 http://deta.qld.gov.au/

APP 10 places obligations on an entity to ensure the quality of personal information it holds, uses and discloses. APP 13 creates obligations to correct personal information if so requested by the subject of the personal information. Both of these APPs refer to accuracy, up-to-dateness and completeness.

The OIC recommends that the Committee consider whether it would be appropriate to include 'misleading' in each of these APPs, to address situations where information may be correct, up-to-date and complete, but may still create a misleading impression in the mind of a reader. There is a distinction between a misleading impression and an inaccuracy, although there will often be significant overlap; inaccurate facts may well be misleading. However, accurate facts may also give a misleading impression, either because they are incomplete or because the language used in recording the facts could convey a misleading impression.

Section 15 - solicited and non-solicited personal information

Section 15 sets out that an entity solicits personal information if the entity *requests* a person to provide the personal information, or to provide a kind of information in which that personal information is included. APP 3 regulates what personal information an agency may solicit; APP 4 regulates unsolicited information.

The presumption could be made that anything which is not captured by the definition of solicit in section 15 will be considered unsolicited information and treated as such under the relevant APPs.

There are a number of methods by which an entity may collect personal information that appears to fall outside the definition of solicit, but which could not properly be said to result in unsolicited information. This would include personal information collected in a passive way by an entity, such as through the use of CCTV cameras or automated tools that track and record internet usage, or information collected on forms which are provided by the entity for individuals to complete - for example forms hosted on the entity's website.

In the case of passive collection, the entity has not directly asked any individual to give it personal information, but the individual can not be said to have provided their personal information unsolicited to the entity. The entity has collected it by way of observation, whatever the means, and generally the individual would have no choice as to whether it was provided to the entity or not; it is beyond their control.

In the case of forms produced by the entity: the entity has not actively asked the individual for the personal information they will provide on the form, but, by producing the forms, which themselves may contain questions, the entity has, at the least, invited the individual to give this personal information to the entity. Again, this cannot precisely be said to be unsolicited information.

The OIC recommends that the Committee consider whether the definition of solicit should be expanded to include situations such as those in which an agency collects personal information by observing the individual or by providing an opportunity for the individual to provide it to the agency.

Generally Available Publications

The definition of 'generally available publication' in section 15 provides that a generally

available publication means a magazine, book, article, newspaper or other publication that is or will be generally available to the public, regardless of the form in which it is published or any fee payable to acquire it. Generally available publications are exempt from the rules about use and disclosure contained in APP 6.

The OIC agrees with the clarification that a fee payable does not preclude a publication from being considered generally available. There are, however, three issues relating to this definition that the OIC believes could benefit from further consideration:

a) *Will be* available to the public

The OIC questions whether it is appropriate to include this in the definition of generally available publication. The reasoning behind excluding generally available publications from privacy principles appears to be predicated on the fact that anyone can access them. As such, there is no benefit to be gained from requiring entities to protect them in the same way they protect information which is not available to the public. Including publications which will be, but are not yet, available to the public in the definition of generally available publication appears to be inconsistent with this reasoning. It could also result in a situation in which personal information is not protected because it is intended to be made public, but the intention is never realised. The OIC would recommend the Committee consider whether it is appropriate to include publications not yet available to the public in this definition.

b) Lawful

The OIC would welcome consideration of whether or not the lawfulness of any inclusion of personal information in a publication has a bearing on whether or not that publication can be considered a generally available publication. For example, if an entity places personal information on a webpage on its website, that webpage would be a generally available publication based on the definition in section 15. However, if an entity had no authority to include that personal information on the webpage, and had breached the obligation to comply with the privacy principles by doing so, would that arguably unlawful action mean that the entity could avoid any further use or disclosure obligations in relation to that personal information? It seems contrary to the spirit of information privacy legislation to allow an entity to avoid its ongoing privacy obligations as a result of a privacy breach. The OIC recommends the Committee consider this issue and whether it would be appropriate to provide clarification around it in the definition of generally available publication.

c) Databases

The definition of generally available publication includes a magazine, book, article, newspaper or other publication. While this is not an exhaustive definition, the provided examples appear to create a specific class of publications which could exclude databases. Where an entity maintains a database or public register which is lawfully available to the general public— for example, the States and Territories maintain property title databases which are searchable by any member of the general public for a fee—there seems no reason to exclude them from the definition of generally available publication. However, it is not apparent that they would be included in this definition. The OIC recommends the Committee consider whether

databases should be specifically referenced in the definition of generally available publication.

Small business exemption

OIC acknowledges that the Commonwealth Government has yet to definitively decide whether the 'small business exemption' will be retained in the final iteration of the new Privacy Act. OIC also acknowledges that a discussion of this exemption is outside the current consideration of the APPs.

Nonetheless, OIC takes this opportunity to argue against the retention of the small business exemption for the following reasons.

It is an oft-quoted truism that today's smart phones are more powerful than the computers that enabled humanity to reach the moon. There would not be a small business today that did not use computer systems, greater or smaller, connected to the internet with the capacity to collect, use and disclose relatively vast amounts of personal information. In other words, in terms of data management, the label of 'small business' no longer has meaning.

The community is particularly vulnerable to a privacy breach by small business. A 2009 study found that 1/3 of all privacy breaches involved outsourced data to third parties[2]. With government entities, this means when personal information is passed onto the private and community sectors.

At present, except in limited circumstances[3] there is no privacy protection applying when a State entity outsources services involving personal information to the private sector. OIC respectfully submits that this protection should be available through the Commonwealth's Privacy Act.

2 2009 Annual Study: Australian Cost of a Data Breach Understanding Financial Impact, Customer Turnover, and Preventative Solutions 2009 Ponemon Institute Benchmark Study (sponsored by PGP Corporation).

3 Part 4 of the *Information Privacy Act 2009* (Qld) obligates a State entity to take all reasonable steps to contract private sector organisation to compliance with the privacy principles.