Office of the Information Commissioner
Queensland

Submission to the Department of Justice and Attorney-General Discussion Paper

Review of the Information Privacy Act 2009

November 2013

Table of Contents

EXECUTIVE SUMMARY

The Office of the Information Commissioner (OIC) welcomes the opportunity to comment on the legislative review of the *Information Privacy Act 2009* (IP Act). As the objects of the review include investigating any specific issue recommended by the Information Commissioner OIC provided key issues to the Department of Justice and Attorney-General in June 2011 and March 2013.

A primary object of the IP Act is to 'provide for the fair collection and handling in the public sector environment of personal information'. Overall, OIC considers that the IP Act effectively meets this objective. Fairness is delivered by striking an appropriate balance between enabling the legitimate business of government, including provision of community services, and providing robust protections against the misuse of personal information. OIC's experience over the last four years is that the privacy principles have, for the most part, struck this balance.

The IP Act provides a flexible roadmap that guides agencies in appropriately protecting the community's personal information while ensuring government can effectively carry out its business. The recommendations in this submission are targeted at refining or adjusting the privacy principles so their application is more certain and the minimum compliance burden is imposed on agencies without compromising privacy protections currently enjoyed by the community.

OIC has observed that most agencies have readily adopted the IP Act's privacy protections. OIC performance and monitoring activities have found that there has been an improvement in reported compliance with obligations across all agencies since the first self-assessed Electronic Audit in 2010, with over 85% agencies reporting that they have now fully or partially implemented their obligations under the IP Act. Similarly, OIC desktop audits of agency websites in 2012-13 show that agencies have continued to improve online compliance in relation to the collection of personal information and provision of information about agency documents containing personal information.

OIC's submission provides feedback on specific issues raised by the discussion paper. It also addresses issues which OIC has identified in over four years of the IP Act's operation, arising out of OIC's performance monitoring, privacy complaint mediation, training and information and assistance functions.

In this submission OIC provides twenty-two recommendations which are, for the most part, minor, to streamline and improve the operation of the legislation. The overarching theme of OIC's recommendations is the need for consistency, with a focus on reducing the administrative burden of the IP Act and simplifying mechanisms which, in practice, have proved to be unnecessarily complex.

OIC believes that the suggested changes will improve privacy practices in agencies, simplify compliance, and improve certainty for the community. OIC also believes these suggested changes will increase the flexibility of the IP Act to deal with the move to provide government services in an online environment, utilise cloud services to decrease costs, and outsource government functions to contracted service providers.

SUMMARY OF OIC RESPONSES TO THE LEGISLATIVE REVIEW OF THE IP ACT

1. Recommendation one: OIC recommends developing a single set of privacy principles based on the IP Act's National Privacy Principles rather than adoption of the APPs. OIC also recommends, in the interests of simplifying compliance, incorporating section 33 of the IP Act into these privacy principles.

2. Recommendation two: If a single set of principles is not adopted, OIC recommends amending the Act so the privacy principles apply to all personal information in the same way, regardless of the agency which holds it, by amending the IPPs to remove the requirement that personal information be contained in a document.

3. Recommendation three: OIC recommends amending schedule 1 to exclude personal information arising out of the circumstances listed in schedule 1 rather than documents.

4. Recommendation four: OIC recommends amending IPP 2(2) to omit the words 'asks the individual' and replace them with the wording from NPP 1: 'collects personal information about the individual from the individual'. OIC also suggests making the same amendment to IPP 3(2). OIC notes, however, that this issue would be resolved by unifying the IPPs and NPPs into the QPPs.

5. Recommendation five: OIC recommends improving the information sharing rules by adopting a single set of privacy principles based on the NPPs for Queensland government agencies. Alternatively, OIC recommends amending IPPs 10 and 11 so that the same information sharing rules apply to all Queensland agencies.

6. Recommendation six: OIC recommends amending IPPs 10 and 11 and NPP 2 (or the equivalent QPP should the IPPs and NPPs be amalgamated into a single set of QPPs) to permit:
   - an agency to use and disclose personal information where that use or disclosure is reasonably necessary for the purposes of enabling a bound contracted service provider to fulfil the obligations of their contract; and
   - a bound contracted service provider to use personal information and disclose it to the contracting agency where it is reasonably necessary to fulfil the obligations of their contract.

7. Recommendation seven: Other than as noted above OIC does not recommend modifying the rules in the IP Act which allow information sharing. Section 157 (waiver or modification of the privacy principles) is sufficient to effectively deal with unique situations not covered by the information sharing rules set out in the IP Act.

8. Recommendation eight: OIC recommends amending the definition of personal information to reflect the definition in the Commonwealth Privacy Act.

9. Recommendation nine: No recommendation. However OIC notes that GOCs are bound by the Privacy Act which provides similar obligations to the IP Act.

10. Recommendation ten: OIC recommends amending section 33 to regulate 'disclosure' of information out of Australia rather than 'transfer' out of Australia.

11. Recommendation eleven: OIC recommends investigating incorporating Victoria's Information Privacy Principle 9 into section 33 of the IP Act.

12. Recommendation twelve: OIC considers that the accountability approach is already in effective operation in Queensland and does not recommend amending the Act. OIC notes that regulating disclosure rather than transfer overseas will strengthen the effective operation of the accountability approach.

13. Recommendation thirteen: OIC recommends amending the Act to remove the 45 business day time frame before complaints can be brought to OIC and replace it with a discretion to accept privacy complaints based on specific circumstances.

14. Recommendation fourteen: OIC recommends the introduction of mechanisms to refine and streamline Chapter 5 of the IP Act. OIC suggests the complaint provisions in the *Information Privacy Act 2000* (Vic) could be adapted in Chapter 5 of the IP Act.

15. Recommendation fifteen: OIC recommends amending the Act to provide the Information Commissioner with a general power to investigate compliance matters.

16. Recommendation sixteen: OIC recommends that section 196(1)(b) and related definitions be amended, consistent with OIC's recommendations in the RTI discussion paper that section 25 of the RTI Act (and consequentially section 45 of the IP Act), to remove provisions which specifically enable a parent to act on behalf of a child so that the general agency provisions will apply.

17. Recommendation seventeen: OIC recommends amending schedule 1, section 7 of the IP Act to exclude both the document and the information it contains from the privacy principles where the document is a generally available publication.

18. Recommendation eighteen: OIC recommends removing the words 'or is to be made' from the definition of generally available publication.

19. Recommendation nineteen: OIC recommends adding emails in transit to schedule 1, section 7 of the IP Act.

20. Recommendation twenty: OIC recommends amending IPP 4 to require an agency to take reasonable steps to protect information. OIC suggests that this could best be achieved by amending IPP 4 to mirror NPP 4. OIC notes that this issue would be resolved by unifying the IPPs and NPPs into a consistent set of privacy principles based on the NPPs.

21. Recommendation twenty-one: OIC recommends amending Sections 28 and 32 of the IP Act to:
    - require personal information to be directly connected with, or directly relevant to, personal information published or provided for publication by the individual
    - require a public interest assessment to be made before an agency is entitled to disregard the specified privacy principles. Wording similar to that in section 157(4) could be used, for example: "An agency must be satisfied that the public interest in not complying with the specified privacy principles outweighs the public interest in complying with them in relation to personal information…"
    - remove IPP 8 and NPP 3 from the specified privacy principles; and
    - include section 33 in the specified privacy principles.

22. Recommendation twenty-two: OIC recommends investigating a mechanism to remove a bound contracted service provider's ability to refuse to give access to, or amend, personal information under the privacy principles.

THE OFFICE OF THE INFORMATION COMMISSIONER

The statutory role of the Information Commissioner under the IP Act is to independently review decisions made by Queensland Ministers, public sector agencies and public authorities about access to, or amendment of, documents, resolve privacy complaints through mediation, promote information rights and responsibilities, and foster improvements in the quality of RTI and information privacy practice in agencies. The Privacy Commissioner and Right to Information Commissioner perform the role of deputy to the Information Commissioner and are delegated powers under the IP Act.

OIC functions include conducting external reviews of agency decisions, monitoring agency performance under the *Right to Information Act 2009* (RTI Act) and IP Act, mediating privacy complaints, deciding applications for waiver of the privacy principles, and providing information and assistance to agencies and the public. There is synergy between all functions of the Office, as the activities of one function support and complement the work of another.

From 1992 until July 2009 OIC's role under the repealed *Freedom of Information Act 1992* (FOI Act) was to conduct independent external reviews of decisions, including about access to documents. The IP Act expanded OIC's functions, creating the role of Privacy Commissioner and giving the Office new functions to support compliance with the privacy principles and protection mechanisms.

PRIVACY IN QUEENSLAND

In June 1997, the Legal, Constitutional and Administrative Review Committee (LCARC) tabled *Privacy in Queensland*, a report which detailed the findings of their extensive review of privacy in Queensland. LCARC recommended the establishment of a privacy regime in Queensland, which would include Information Privacy Principles that would be based on the Information Privacy Principles in the *Privacy Act 1988* (Cth)[1], and a Privacy Commissioner who would be a Parliamentary Officer.

In 2001, Information Standard 42 (IS42) and Information Standard 42A (IS42A)[2] were introduced, applying to departments, statutory bodies, and some GOCs; neither applied to local government[3]. The Information Standards were based on the Privacy Principles in the Commonwealth *Privacy Act 1988* (Privacy Act). IS42 and IS42A required agencies to follow the privacy principles, appoint a privacy officer, publish a privacy plan and develop privacy complaint resolution mechanisms.

The *Information Privacy Act 2009* arose out of 2008's *Independent Review of Freedom of Information in Queensland*, conducted by the Independent FOI Review Panel chaired by Dr David Solomon (the Panel). The Panel considered the interaction between freedom of information and privacy and

[1] Note that the National Privacy Principles did not yet exist as part of the *Privacy Act 1988*.
[2] IS42A applied only to Queensland Health and was based on the National Privacy Principles in the Privacy Act.
[3] IS42 was issued under the authority of ss. 22(2) and 56(1) of the *Financial Management Standard 1997* and applied to accountable officers of departments and statutory bodies (local government was explicitly excluded from the definition of 'statutory body'). GOCs were only captured if the shareholding Minister gave a notice to that effect. IS42A only applied to the Queensland Department of Health.

recommended the creation of a separate privacy regime and the creation of a privacy commissioner to help safeguard and promote privacy rights[4].

[4] *The Right to Information: Reviewing Queensland's Freedom of Information Act* page 45

CONSISTENCY

1.0 What would be the advantages and disadvantages of aligning the IPPs with the APPs, or adopting the APPs in Queensland?

13.0 Should the reference to documents in the IPPs be removed; and if so, how would this be regulated?

Recommendation one: OIC recommends developing a single set of privacy principles based on the IP Act's National Privacy Principles rather than adoption of the APPs. OIC also recommends, in the interests of simplifying compliance, incorporating section 33 of the IP Act into these privacy principles.

Recommendation two: If a single set of principles is not adopted, OIC recommends amending the Act so the privacy principles apply to all personal information in the same way, regardless of the agency which holds it, by amending the IPPs to remove the requirement that personal information be contained in a document.

Recommendation three: OIC recommends amending schedule 1 to exclude personal information arising out of the circumstances listed in schedule 1 rather than documents.

Consistency of privacy principles

Adopting a single set of privacy principles in Queensland would ensure consistency of privacy obligations across all Queensland government agencies. Currently, this consistency does not exist.

The Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) create two separate sets of privacy obligations and privacy rights under the IP Act. The NPPs apply to health agencies; the IPPs apply to all other agencies.

OIC submits that having two sets of privacy principles creates unnecessary confusion for the community and inconsistency between agencies. It also necessitates double-handling for whole of government privacy resources, for example, whole of government privacy training such as that produced by the OIC. It also creates the situation where government employees who move from a health agency to another agency or vice versa have to relearn the privacy rules with which they must comply.

The existence of two different sets of principles also impacts on whole of government contractors. Under Chapter 2, part 4 of the IP Act contractors can be bound to comply with the privacy principles[5]. Health agencies bind their contractors to the NPPs; all other agencies bind their contractors to the IPPs. This means different obligations will apply to the contractor depending on which agency they contract with.

OIC considers that a single set of privacy principles which applied to all Queensland government agencies would eliminate these issues. As part of simplifying compliance, OIC suggests that section 33, which is a privacy principle as defined in schedule 6 of the IP Act, be included in the single set of privacy principles, rather than remaining as a section in chapter 2.

[5] In the circumstances set out in Sections 34 and 35 of the IP Act.

Information versus documents

The IPPs do not apply to personal information generally; they only apply to personal information contained in a document. Conversely, the NPPs apply to all personal information, regardless of whether or not it is contained in a document.

Health agencies are required to comply with the NPPs while all other agencies are required to comply with the IPPs. This means that, for example, personal information provided verbally to an officer of a non-health agency is not protected by the IP Act; if the officer belonged to a health agency, the personal information would be protected by the IP Act. OIC submits that privacy protections should be consistent across all Queensland agencies.

The NPPs have never required personal information to be contained in a document before their protections apply. OIC has not encountered any issues with regulating, implementing or supporting health agency compliance arising from there being no requirement that personal information be contained in a document. As such, OIC does not anticipate that regulation of the IPPs with the document requirement removed would present any difficulties.

APPs or a single set of Queensland Privacy Principles

The APPs grew out of recommendations made by the ALRC in Report 108 *For Your Information: Australian Privacy Law and Practice* (the Report), which was the culmination of a twenty-eight month inquiry into the *Privacy Act 1988* (Cth). This inquiry considered the extent to which the *Privacy Act 1988* and related laws provided an effective privacy protection framework for Australia and canvassed the issue of national consistency.

The threshold issue considered by the ALRC was whether or not national consistency was important. Numerous stakeholders submitted to the review that it was, identifying the inconsistency of privacy regulation of the private sector, including the private health sector, as the cause of unnecessary compliance burden and expense.

The ALRC concluded that inconsistent privacy regulation does cause problems and that national consistency should be one of the goals of privacy regulation. However, OIC notes that the majority of issues raised by submitters to the review involved the inconsistency of private sector privacy laws; the Report does not discuss difficulties associated with different privacy laws applying across the public sectors before recommending national consistency.

The APPs are intended to apply to the diverse ranges of entities subject to the *Privacy Act 1988* (Cth), including private entities with a turnover in excess of three million dollars per year, health care providers, and Commonwealth government agencies. The APPs have had to cater for these entities' differing priorities and areas of operation. In contrast, Queensland's IP Act applies only to Queensland government agencies. This has allowed the IP Act to have a degree of specificity tailored to the particular needs and operations of government.

The APPs do not come into force until March 2014. This means that at this time they are untested and untried. As the APPs become operational, their interpretation and practical application will be subject to debate and possibly amendment. If the Queensland Government were to adopt the APPs, it would similarly adopt the uncertainty that will be associated with them until they are understood and 'bedded in'.

While there are strong similarities between all privacy principles, some of the APPs may have lesser relevance[6] to Queensland government agencies, given they have been drafted to apply to both the private and public sector. As noted above, adoption of the APPs at this point would require Queensland government agencies to familiarise themselves with, and adapt their processes to, an entirely new set of privacy principles.

OIC agrees that simplification would have a positive impact on agency compliance and potentially reduce agencies' corresponding administrative burden. However, adopting the APPs is likely to introduce uncertainty regarding government agency obligations, with new principles better suited to the private sector.

OIC's experience is that agencies have worked hard over to the last four years to develop a strong familiarity, and corresponding high level of compliance, with their existing privacy obligations, particularly local government, which had not previously been subject to privacy regulation. As agencies move to new avenues of service delivery and explore new business methods they are readily incorporating privacy principles into their new working practices. This is demonstrated by the discussions relating to Government's recent moves to offer higher levels of digital service delivery and the success and expansion of the Open Data scheme.

OIC suggests that, at this time, a move to adopt the APPs would impose an administrative burden on agencies as they would have to develop a similar familiarity with the new principles, and adapt them to their new working practices, without the extensive guidance OIC is currently able to provide.

OIC suggests that, rather than adopting the APPs in Queensland, it would be preferable to align the IPPs with the NPPs by amalgamating them into a single set of principles based on the NPPs: the Queensland Privacy Principles or QPPs.

While there are differences between the IPPs and NPPs which would require a minor period of adjustment if Queensland moved to amalgamated QPPs, in most cases these differences are relatively minor; the NPPs *simplify* obligations contained in the IPPs rather than change them. This is demonstrated by the Discussion Paper itself, which discusses issues relating solely to the IPPs because those issues are simply not present in the NPPs[7].

OIC suggests the adoption of QPPs would have a positive impact on agencies' privacy compliance burden and would impose a relatively short period of adjustment and a correspondingly small expenditure of resources for the transition.

[6] For example - APP 7 is solely concerned with the direct marketing activities of entities, much of which would arguably have little applicability to government agencies.
[7] See, for example, the discussion on the security obligations in IPP 4 at Question 14.0.

Schedule 1: documents but not information

Schedule 1 of the IP Act lists documents to which the privacy principles do not apply. These are documents which arise out of the specific situations set out in schedule 1. For example, schedule 1, section 3 of the IP Act excludes a document to the extent it contains personal information arising out of a complaint under the *Police Service Administration Act 1990*, part 7 or a complaint, or an investigation of misconduct, under the *Crime and Misconduct Act 2001*. To be excluded under this section the document itself must have arisen out of the complaint investigation; only the document, not the personal information within it, is excluded from the privacy principles. This creates the situation where information extracted from the excluded document is once again subject to the privacy principles.

OIC suggests that schedule 1 be amended to exclude the personal information which arises out of these situations, rather than the documents.

15.0 Should the words 'ask for' be replaced with collect for the purposes of IPPs 2 and 3?

Recommendation four: OIC recommends amending IPP 2(2) to omit the words 'asks the individual' and replace them with the wording from NPP 1: 'collects personal information about the individual from the individual'. OIC also suggests making the same amendment to IPP 3(2). OIC notes, however, that this issue would be resolved by unifying the IPPs and NPPs into the QPPs.

Information Privacy Principle 2 (IPP 2) requires an agency to provide certain information to an individual when it *asks* that individual for their personal information. Conversely, National Privacy Principle 1 (NPP 1) requires health agencies to provide certain information to an individual when it *collects* personal information about the individual from the individual.

The use of the word 'asks' in IPP 2(2) has created confusion amongst agencies about when the requirements in IPP 2 apply. One interpretation is that IPP 2 applies only when an agency actively obtains information on a personal level. Another interpretation is that it also includes indirect collection, for example through an online agency forms. A broader interpretation is that IPP 2 applies to any collection of information from the individual, including purely passive collections such as CCTV recording.

It does not appear to be consistent with the objects of the IP Act that personal information would be covered by IPP 2 if an officer hands an individual a form and asks them to fill it out, but would not apply to the same form discovered online and completed by the individual.

OIC notes that NPP 1, which governs collection of personal information by health agencies, does not present this issue as it refers to collection rather than using the word ask.

This confusion creates uncertainty for agencies, individuals, and the OIC, particularly in relation to its monitoring and support functions. Additionally, OIC considers that it is appropriate that privacy protections apply to all personal information collected from individual by an agency, regardless of the agency which collects it or the circumstances under which the information was collected.

SHARING INFORMATION

2.0 Does the IP Act inappropriately restrict the sharing of information? If so, in what ways? Do the exceptions need to be modified?

Recommendation five: OIC recommends improving the information sharing rules by adopting a single set of privacy principles based on the NPPs for Queensland government agencies. Alternatively, OIC recommends amending IPPs 10 and 11 so that the same information sharing rules apply to all Queensland agencies.

Recommendation six: OIC recommends amending IPPs 10 and 11 and NPP 2 (or the equivalent QPP should the IPPs and NPPs be amalgamated into a single set of QPPs) to permit:

- ***an agency to use and disclose personal information where that use or disclosure is reasonably necessary for the purposes of enabling a bound contracted service provider to fulfil the obligations of their contract; and***
- ***a bound contracted service provider to use personal information and disclose it to the contracting agency where it is reasonably necessary to fulfil the obligations of their contract.***

Recommendation seven: Other than as noted above OIC does not recommend modifying the rules in the IP Act which allow information sharing. Section 157 (waiver or modification of the privacy principles) is sufficient to effectively deal with unique situations not covered by the information sharing rules set out in the IP Act.

The IP Act does not limit the *entities* with whom information can be shared. Rather, it regulates the *situations* in which information can be shared. The circumstances in which an agency is permitted to share personal information with a third party include the following:

- Where it is necessary for law enforcement activities[8].
- Machinery of Government changes brought about by an Administrative Arrangements Order or other legislation.
- Minimising threats to individuals or to the public, such as dealing with emergency or disaster situations.
- Briefing Ministers in relation to their portfolio responsibilities.
- Responding to or discussing personal information published by the individual.
- Where the individual consents to the sharing or was made aware when the information was collected that the information sharing was going to occur.
- Where the sharing is authorised or required by law.

These rules are set out in the Information Privacy Principles, National Privacy Principles, and Chapter 2 of the IP Act. OIC's experience is that the privacy principles have sufficient flexibility to allow the flow of information for legitimate purposes. The capacity of OIC to grant applications for waiver and

[8] Including criminal offences, breaches of laws which impose penalties or sanctions, proceeds of crime laws, public revenue protection, seriously improper conduct breaches, and preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

modification (see following discussion) caters for exceptional circumstances. However, OIC acknowledges that some minor refinement could provide certainty for agencies.

Information sharing in a consistent model

As discussed in response to Questions 1.0, 13.0 and 15.0, OIC supports the adoption of a consistent set of privacy principles, based on the NPPs, which apply to all Queensland government agencies – the QPPs.

There are minor differences between when the IPPs allow personal information to be used for a secondary purpose and when they allow it to be disclosed. OIC's experience is that these differences have little to no practical impact. OIC notes that the NPPs have the same rules for use of personal information for a secondary purpose and disclosure of personal information. OIC's view is that a simpler consistent regime is preferable to one where different rules apply to different agencies.

Outsourcing arrangements and disclosure

Chapter 2, part 4 of the IP Act can require a service provider to be bound to comply with the obligations in the privacy principles as if it were the government agency. If an agency outsources one or more of its functions and this will involve the movement of personal information the agency must comply with chapter 2, part 4. If bound, the service provider is referred to as a 'bound contracted service provider'. In this way, the IP Act supports the outsourcing of government services.

However, where outsourcing arrangement will involve personal information, there can be difficulties. The transfer of personal information to the service provider may be a disclosure, but this is not contemplated by the disclosure rules in the IPPs or NPPs. Preparing the personal information or transfer may be a secondary use of personal information, but this is not contemplated by the use rules in the IPPs or NPPs.

OIC suggests that it would be appropriate to amend the IPPs and NPPs (or include in the QPPs if adopted) to permit the use and disclosure of personal information where it is a necessary part of complying with a contract where the contractor is a bound contracted service provider.

Waiver and modification

Section 157 of the IP Act allows an agency to apply to OIC for a waiver or modification of the privacy principles in situations where the principles are preventing an agency's activities. In order to be granted, non-compliance, or complying in a different way, with the privacy principles must outweigh the public interest in complying with the privacy principles as they appear in the IP Act.

Since July 2009, OIC has received only six formal applications under section 157 for a waiver of the privacy principles. All of these applications were made because the agency considered that it was in a unique situation which could not be reconciled with the existing privacy principles. Decisions giving an approval for a waiver or modification of privacy principles are published on OIC's website.

DEFINITION OF 'PERSONAL INFORMATION'

3.0 Should the definition of personal information in the IP Act be amended to bring it into line with the definition in the Commonwealth *Privacy Amendment Act 2012*?

Recommendation eight: OIC recommends amending the definition of personal information to reflect the definition in the Commonwealth Privacy Act.

The definition of personal information in the IP Act is "information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion"[9].

Given the reference to 'information or opinions in a database', this definition appears to be archaic, dating from a time when databases were not common. It is also cumbersome and would benefit from amendment that streamlines and clarifies the definition.

OIC notes that the definition of personal information in the IP Act is not only used for the privacy principles. It is also used for Chapter 3 of the IP Act, which contains access and amendment rights, and for the *Right to Information Act 2009* (RTI Act)[10].

OIC agrees that amending the definition of personal information to replicate the Commonwealth definition would not significantly change the scope of personal information in Queensland for the privacy principles. OIC notes that the amendment does not appear to create any negative consequences for applications under the IP Act or RTI Act, nor for the application of the RTI Act public interest factors which refer to personal information.

[9] Section 12, IP Act
[10] Schedule 6, RTI Act, definition of personal information

QUEENSLAND GOCS

4.0 Should government owned corporations in Queensland be subject to the Queensland IP Act or should they continue to be bound by the Commonwealth Privacy Act?

Recommendation nine: No recommendation. However OIC notes that GOCs are bound by the Privacy Act which provides similar obligations to the IP Act.

Schedule 2 of the IP Act states that a government owned corporation (GOC) or a subsidiary of a government owned corporation is not subject to the privacy principles. A GOC is an entity to which the privacy principles do not apply.

OIC notes that GOCs are subject to the *Privacy Act 1988* (Commonwealth). Given that the GOCs operate in a commercial environment OIC suggests that it may be appropriate that they continue to be bound by the Privacy Act, which provides a similar level of protection for the community in relation to handling and use of their personal information.

TRANSFERRING PERSONAL INFORMATION OUT OF AUSTRALIA

5.0 Should section 33 be revised to ensure it accommodates the realities of working with personal information in an online environment?

6.0 Does section 33 present problems for agencies in placing personal Information online?

Recommendation ten: OIC recommends amending section 33 to regulate 'disclosure' of information out of Australia rather than 'transfer' out of Australia.

Recommendation eleven: OIC recommends investigating incorporating Victoria's Information Privacy Principle 9 into section 33 of the IP Act.

Section 33 is the privacy principle that regulates overseas transfer of personal information. It has ben OIC's experience that, as it is currently formulated, it is of limited utility when working in an online environment.

Regulating transfer

Section 33 of the IP Act regulates the *transfer* of personal information out of Australia. The word transfer is not defined in the IP Act.

Transfer in this context means the act of sending information from Australia to another country, regardless of who retains control of the information. For example, faxing a document from Queensland to an agency officer travelling overseas on agency business would constitute a transfer which would have to comply with section 33, as would that same officer travelling out of Australia with agency files or computer equipment containing personal information.

OIC suggests that the use of the word *transfer,* which has a very broad meaning, can not only create unnecessary complexity but also produce outcomes that defy common sense[11]. *Transfer* is simply the movement of personal information; it requires the same level of compliance activity regardless of whether or not the agency retains control of the information and has no regard to the content of the information.

Disclosure is defined in section 23 of the IP Act: information is disclosed if the entity the information is being given to does not know it and is not in a position to find it out and the agency ceases to have control of the information. OIC submits that regulating the *disclosure* of personal information out of Australia rather than transfer would be more appropriate.

OIC notes that one of the recent changes to the Privacy Act was to substitute disclosure for transfer in its equivalent provision to section 33. [12]

The Victorian model

In addition to amending section 33 to regulate disclosure rather than transfer, OIC suggests that section 33 could be generally amended to increase its flexibility. The *Information Privacy Act 2000* (Vic) regulates the flow of personal information outside of Victoria. OIC does not support amending

[11] For example, sending an individual their own personal information while they are overseas would constitute a transfer out of Australia and could require compliance with section 33. If they had not consented to receive it, the agency could be in breach of section 33.
[12] See APP 8.1

section 33 to regulate flow of information outside of Queensland, however Information Privacy Principle 9 (Vic) contains provisions which, if imported into Queensland's IP Act, could make section 33 sufficiently flexible to deal with both the online and offline environment.

IPP 9 (Vic) allows information to be transferred in a number of circumstances that are not catered for in section 33. OIC suggests that it is more responsive to the day-to-day business requirements of agencies. Factors which permit transfer in IPP 9 (Vic) include that the recipient is subject to privacy regulation substantially similar to the IPPs or that the organisation transferring has taken reasonable steps to ensure that it will not be held, used, or disclosed in a manner inconsistent with the IPPs. Additionally, IPP 9 (Vic) specifically permits transfer which is necessary for the performance of contracts and pre-contractual measures relating to the individual.

Another significant difference between Victoria's IPP 9 and Queensland's section 33 is the former requires the agency to satisfy only one set of conditions whereas the IP Act's equivalent provision – section 33(d) – requires two sets of conditions to be satisfied.

Unlike IPP 9 (Vic), section 33 allows information to be transferred where authorised or required by law or necessary to lessen or prevent a serious threat to health and safety. OIC recommends retaining these if section 33 were to be amended to reflect the Victorian approach.

7.0 Should an accountability approach be considered for Queensland?

Recommendation twelve: OIC considers that the accountability approach is already in effective operation in Queensland and does not recommend amending the Act. OIC notes that regulating disclosure rather than transfer overseas will strengthen the effective operation of the accountability approach.

The accountability principle discussed in the Australian Law Reform Commission's Discussion Paper 72 involved providing that agencies and organisations continue to be liable for any breaches of the privacy principles when an individual's personal information is transferred outside Australia.[13] ALRC stated that "an agency or organisation should not be liable for the handling of personal information after it has been transferred to another entity when the individual in question consents to the transfer."[14]

As noted in the Discussion Paper, the ALRC supported that an agency should not be accountable if the information is being sent to a jurisdiction with effective privacy regulation, the individual has provided informed consent to the transfer, or the transfer was authorised or required by law.

OIC suggests that, in effect, the accountability approach is already in use in Queensland. An individual is able to make a complaint about, or the Information Commissioner to take compliance action against, an agency which has breached the privacy principles. The definition of privacy principle in schedule 5 of the IP Act includes section 33. Section 33 allows an agency to transfer information out of Australia in compliance with section 33, which means if the agency does so, the

[13] Paragraph 28.65 http://www.austlii.edu.au/au/other/alrc/publications/dp/72/28.html#Heading143
[14] Paragraph 28.69 http://www.austlii.edu.au/au/other/alrc/publications/dp/72/28.html#Heading143

agency has not breached the privacy principles and is no longer accountable for what happens to the information.

This will be strengthened by amending section 33 to govern disclosure rather than transfer, as the definition of disclosure requires the agency to cease to have control of the information.

OIC does not see any compliance advantage to specifying in section 33 that an agency ceases to be responsible for information transferred in reliance on section 33, however it may provide certainty for agencies or individuals.

PRIVACY COMPLAINTS

Recommendation thirteen: OIC recommends amending the Act to remove the 45 business day time frame before complaints can be brought to OIC and replace it with a discretion to accept privacy complaints based on specific circumstances.

Recommendation fourteen: OIC recommends the introduction of mechanisms to refine and streamline Chapter 5 of the IP Act. OIC suggests the complaint provisions in the Information Privacy Act 2000 (Vic) could be adapted in Chapter 5 of the IP Act.

8.0 Should the IP Act provide more detail about how complaints should be dealt with?

Chapter 5 of the IP Act deals with complaints about a breach of the privacy principles. It provides very little detail on how complaints are to be made to, or dealt with by, an agency. Section 166(3)(a) requires an individual to have first complained to 'an appropriate person within the relevant entity under the complaint management system of the relevant entity'. Section 166(3)(b) effectively gives an agency a minimum period 45 business days to resolve a privacy complaint.

It is OIC's experience that agencies and complainants benefit from flexibility in the management of privacy complaints. OIC notes that the Discussion Paper refers to the prescriptive nature of Chapter 3 of the IP Act, which deals with applications for access and amendment, as a comparison for the non-prescriptive nature of Chapter 5 as it applies to agency processes. It is OIC's view that these two processes are not directly comparable and Chapter 3 should not serve as a basis for how agencies are required to deal with privacy complaints.

9.0 Should the IP Act provide more flexibility about the timeframe for complaints to the OIC to be lodged?

Under section 166(3) of the IP Act before a complainant can bring their privacy complaint to OIC they must give the agency a minimum of 45 business days, to deal with the complaint to the complainant's satisfaction.

These requirements can have two significant but contrasting effects on the management of privacy complaints. The prescriptive nature of this section requires the individual not only to make their complaint to the agency, but to direct it to a specific person within that agency. For example, if the agency has a dedicated person that deals with privacy complaints the complainant is obligated to direct their privacy complaint to them.

A breakdown in this process, such as the complainant failing to direct their complaint to the appropriate person, can result in the agency having the complaint for 45 business days but not necessarily dealing with it as a privacy complaint. If the complainant were to then lodge their privacy complaint with OIC it would have to be remitted back to the agency to deal with as a privacy complaint, at which point the complainant would have to wait another 45 business days. In OIC's experience this is a common occurrence.

Another common circumstance occurs when the agency's appropriate person deals expeditiously with a privacy complaint and provides the complainant with a final decision[15] on their privacy complaint. A complainant who is dissatisfied with the agency's response to their privacy complaint must, despite the agency having (from the agency's perspective) resolved their complaint, wait out the remainder of the 45 business day period before they can bring their complaint to OIC. A complainant who fails to do so will have their complaint declined by OIC and will be advised that they must re-lodge at the 45 business day mark.

Both of these scenarios engender frustration in the complainant: at the system, with the agency, and with OIC. In a jurisdiction that heavily emphasises the informal resolution of complaints, the capacity for the process to be a source of frustration is inimical to the resolution of complaints.

In the 2012–2013 financial year, 33% of privacy complaints lodged with OIC were not accepted because they did not meet the requirements of section 166(3) of the IP Act.

OIC's experience in dealing with privacy complaints has suggested a number of ways the complaint framework could be improved.

Section 164 requires that, for a complaint to constitute a privacy complaint, a breach of an individual's privacy must have occurred. There is no capacity for someone to make a privacy complaint about a program or system that would automatically result in a privacy breach. OIC submits that this is the equivalent of a situation where an employee becomes aware of an obviously unsafe area of their workplace but it cannot be rectified until someone actually suffers a safety incident.

Section 25 of the *Information Privacy Act 2000* (Vic) does not define privacy complaints, but rather provides that an individual whose personal information is, or has at any time been, held by an organisation may complain to the Privacy Commissioner about an act or practice that may be an interference with the privacy of the individual.

OIC suggests that amending the IP Act to reflect the Victorian provision could improve the handling of privacy complaints. If this approach is adopted in Queensland's IP Act, OIC recommends retaining the condition that the individual must first have made their complaint to the agency.

Rather than defining how much time must have passed before a complainant can bring their complaint to the Commissioner, section 29 of the *Information Privacy Act 2000* (Vic) sets outs the circumstances in which the Commissioner can decline a privacy complaint, which include that:

- although a complaint has been made to the Privacy Commissioner about the act or practice, the complainant has not complained to the respondent
- the complainant has complained to the respondent about the act or practice and either-
    - the respondent has dealt, or is dealing, adequately with the complaint; or
    - the respondent has not yet had an adequate opportunity to deal with the complaint

[15] Note that that there is no decision making power in Chapter 5 of the IP Act, however the process of dealing with and resolving a privacy complaint requires an agency to decide whether or not there has been a breach of the privacy principles in relation to the complainant's information.

OIC suggests that this approach allows the most responsive method of dealing with privacy complaints, giving OIC the discretion to accept or decline complaints based on how the agency is dealing with the complaint rather than by reference to an arbitrary time period.

POWERS OF THE PRIVACY COMMISSIONER

10.0 Are additional powers for the Information Commissioner to investigate matters potentially subject to a compliance matter necessary?

Recommendation fifteen: OIC recommends amending the Act to provide the Information Commissioner with a general power to investigate compliance matters.

OIC has not experienced any difficulties with the current compliance powers available to the Information Commissioner. OIC notes that it has not issued a compliance notice during this time. In 2010 OIC conducted the *Review of handling of personal information contained in go cards* under section 135 of the IP Act, but found that it was not necessary to issue a compliance notice in that instance.

However, OIC considers that it would be appropriate to include in the IP Act a general power as exists in section 125 of the RTI Act and the Commonwealth Privacy Act.

PERSON ACTING AS AGENT FOR CHILD

11.0 Should parent's ability to do things on behalf of a child be limited to Chapter 3 access and amendment applications?

Recommendation sixteen: OIC recommends that section 196(1)(b) and related definitions be amended, consistent with OIC's recommendations in the RTI discussion paper that section 25 of the RTI Act (and consequentially section 45 of the IP Act), to remove provisions which specifically enable a parent to act on behalf of a child so that the general agency provisions will apply.

Section 196(1)(a) of the IP Act allows one person to act as an authorised agent for another person, and section 196(1)(b) specifically allows a child's parent to do anything that the child could do if the child were an adult, in relation to an access or amendment application or other matter under the IP Act. Both section 196(1)(a) and (b) allow parents to act on behalf of their children in making a privacy complaint.

OIC notes that in its response to question 6.6 of the discussion paper on RTI and Chapter 3 of the IP Act (RTI discussion paper) that it recommends removing section 25 of the RTI Act. If OIC's recommendation in response to question 2.1 of the RTI discussion paper (that access and amendment rights be moved from the IP Act to the RTI Act), is not followed, OIC also recommends removing section 45 of the IP Act, which equivalent to the RTI Act's section 25.

Section 25 of the RTI Act and section 45 of the IP Act allow for applications to be made by parents on behalf of children. This right is additional to the general rule that an applicant can have another person apply on their behalf. In OIC's experience, the existence of these provisions can cause unneeded complexity, as it involves, among other things, having to assess whether the parent is genuinely applying on behalf of the child. This can be difficult to determine. The majority of the application also require an assessment of the child's best interests, which, again, can be difficult for a decision-maker to determine.

Consistent with its recommendation in the RTI discussion paper, OIC believes that section 196(1)(b) and related definitions should be amended to remove provisions which specifically enable a parent to act on behalf of a child so that the general agency provisions will apply.

GENERALLY AVAILABLE PUBLICATIONS

12.0 Should the definition of generally available publication be changed? Is the Commonwealth provision a useful model?

Recommendation seventeen: OIC recommends amending schedule 1, section 7 of the IP Act to exclude both the document and the information it contains from the privacy principles where the document is a generally available publication.

Recommendation eighteen: OIC recommends removing the words 'or is to be made' from the definition of generally available publication.

Schedule 1 of the IP Act lists documents to which the privacy principles do not apply. Section 7 includes generally available publications. A *generally available publication* is defined in schedule 5 as 'a publication that is, or is to be made, generally available to the public, however it is published'.

OIC suggests that the way generally available publications currently work in Queensland could be improved.

Adopting the Commonwealth model

The Commonwealth definition of a generally available publication is "a magazine, book, newspaper or other publication (however published) that is or will be generally available to members of the public whether or not it is published in print, electronically or in any other form and (b) whether or not it is available on the payment of a fee[16]".

OIC supports including the specifics relating to mode of publication and the payment of a fee. OIC does not support otherwise amending the Queensland definition to reflect the Commonwealth definition. OIC suggests that Queensland definition, based on whether the document is available to the public, provides greater flexibility for agencies.

Documents but not the information

The exclusion of generally available publications from the privacy principles only extends to the *document* which is generally available. If the information is extracted from the document that information is no longer excluded from the privacy principles. This could create a situation where an agency could, for example, publish a scanned copy of a document on their website but if they extracted the information and placed it directly on the website it could be a violation of the privacy principles.

OIC notes that the definition of disclosure[17] provides an agency with some leeway in these or similar circumstances, but only in relation to the disclosure principles. The other privacy principles would arguably still apply. In particular, publishing an extract of a generally available publication on a

[16] Section 6, *Privacy Act 1988*

[17] An agency does not disclose information if the entity it is being given to already knows it or is in a position to find it out.

website could potentially be a breach of section 33 of the IP Act, as discussed earlier in this submission.

Intended to be made

The definition of generally available publication includes publications that are generally available to the public and documents that are intended to be made generally available to the public.

The exclusion of generally available documents (and information, as noted above) from the privacy principles is logical. It would make little sense for an agency to manage a document in accordance with the privacy principles when it is freely available to the public. The same is not true of a document which is intended to be made public but it has not yet happened.

12.1 Exclusion of email in transit from the privacy principles

Recommendation nineteen: OIC recommends adding emails in transit to schedule 1, section 7 of the IP Act.

In addition to excluding generally available publications from the privacy principles, schedule 1, section 7 of the IP Act also excludes a letter or anything else while it is being transmitted by post. When an agency posts a letter it loses control of the letter and the personal information it contains; as such, it is appropriate that the privacy principles do not apply to it.

OIC suggests that a similar exclusion should exist for email while it is being transmitted. When an email is sent it travels out of the agency's network and through a number of routers until it reaches its destination. It is effectively out of the agency's control once it has been sent. These routers may be located in Australia or they may be located overseas. The agency has no capacity to determine the path the email will take on its way to its destination.

REASONABLENESS IN SECURITY MEASURES

14.0 Should IPP 4 be amended to provide, in line with other IPPs, that an agency must take reasonable steps to ensure information is protected against loss and misuse?

Recommendation twenty: OIC recommends amending IPP 4 to require an agency to take reasonable steps to protect information. OIC suggests that this could best be achieved by amending IPP 4 to mirror NPP 4.

OIC notes that this issue would be resolved by unifying the IPPs and NPPs into a consistent set of privacy principles based on the NPPs.

IPP 4(1)(a) currently requires an agency that controls a document containing personal information to ensure that information is protected against loss, unauthorised access, use, modification or disclosure, and any other misuse. IPP 4(2) expands on this definition by requiring the protections in IPP 4(1) to include security safeguards adequate to provide the level of protection that could reasonably be expected to be provided. While IPP 4(2) introduces a level of reasonableness in relation to the security safeguards, IPP 4(1) has no such reasonableness test.

OIC's experience during implementation of the IP Act in mid-2009 was that agency privacy officers expressed significant concerns about the absolute nature of IPP 4(1). OIC notes that the lack of a reasonableness test has the potential to place an unreasonable burden on agencies, potentially making them responsible for a privacy breach that occurs despite the agency making every reasonable effort to protect the information.

OIC also notes that this obligation is not consistent with the obligation on health agencies in NPP 4, which requires a health agency to take reasonable steps to protect information, and health agencies are highly likely to hold extremely sensitive information.

ADDITIONAL ISSUES RECOMMENDED FOR INVESTIGATION
Section 28 and 32 – exclusion of self-published information from the privacy principles

Recommendation twenty-one: OIC recommends amending Sections 28 and 32 of the IP Act to:

- ***require personal information to be directly connected with, or directly relevant to, personal information published or provided for publication by the individual***
- ***require a public interest assessment to be made before an agency is entitled to disregard the specified privacy principles. Wording similar to that in section 157(4) could be used, for example: "An agency must be satisfied that the public interest in not complying with the specified privacy principles outweighs the public interest in complying with them in relation to personal information…"***
- ***remove IPP 8 and NPP 3 from the specified privacy principles; and***
- ***include section 33 in the specified privacy principles.***

When an individual publishes their personal information or provides it for the purposes of publication, for example, they make a Facebook post or write a letter to the editor of a newspaper, Sections 28 and 32 of the IP Act allow an agency to disregard specified privacy principles[18] when dealing with any personal information related to or connected with that which was published or provided to be published.

OIC understands that the purpose of these sections is to allow an agency to correct the public record and so prevent harm which could be caused by inaccurate material being presented to the public, however OIC has found that there a number of concerns raised by this section:

- The connection between the information which was published and the information which the agency is not required to treat in accordance with the specified privacy principles is very tenuous, requiring only connection or relevance, as opposed to a direct connection or direct relevance. This means that an agency can potentially disclose further personal information than that which had been put into the public domain[19] by the individual.

- There is no public interest test which requires an agency to assess the public interest harm caused by dealing with personal information outside of the specified privacy principles compared with the harm caused by the information remaining uncorrected in the public record.

- The exclusion of the privacy principles requiring an agency to take reasonable steps to make sure personal information is accurate (IPP 8 and NPP 3). If personal information is to be used and/or disclosed without regard to the privacy principles—particularly where it is being done to correct errors in the public record—it would seem important that steps be taken to ensure its accuracy.

[18] For Section 28, agencies may disregard Information Privacy Principles 8, 9, 10 or 11; for section 32, health agencies may disregard National Privacy Principles 2, 3 (in relation to use or disclosure), or NPP 9(4).
[19] And not even necessarily in the public domain. Sections 28 and 32 apply at the point where the personal information had simply been given for the purpose of publication.

OIC recognises the importance of Sections 28 and 32, but also recognises that it is important to strike an appropriate balance between agencies' need to use personal information and privacy protections for the community. OIC notes that in their current form Sections 28 and 32 do not appear to find an appropriate balance.

OIC also notes that section 33, which contains the overseas transfer rules, is not included in Sections 28 and 32. This can cause difficulties in some agency interactions with the public. The most common occurrence that OIC has observed is where an agency is interacting with someone on Facebook. Given that Facebook is an American company with a computer infrastructure based in America, entering personal information into a Facebook post requires the agency to transfer it overseas. Section 33 may make this difficult or impossible, depending on the circumstances.

Given the increasing use of social media and other online methods of communication, OIC suggests that it would be appropriate to include section 33 in the list of privacy principles with which an agency need not comply.

Application of IPPs 6-7 or NPPs 6-7 to bound contracted service providers

Recommendation twenty-two: OIC recommends investigating a mechanism to remove a bound contracted service provider's ability to refuse to give access to, or amend, personal information under the privacy principles.

Under Chapter 2, part 4 of the IP Act a private entity contracting with government can be bound to comply with section 33 of the IP Act and the IPPs or the NPPs[20] as if they were an agency, becoming a bound contracted service provider. However, while the privacy principles relating to access and amendment *apply* to them, bound contracted service providers may not be required to give effect to them.

IPPs 6-7 and NPPs 6-7 contain obligations that require agencies to:

- give individuals access to their personal information; and
- allow individuals to amend their personal information.

However, these IPPs and NPPs contain exceptions:

- an agency is not required to give access to personal information under IPP 6 or NPP 6 if, under an access law of the State, it would be authorised or required to refuse access[21]; and
- the right to amend in IPP 7 and NPP 7 applies subject to any limitation in a State law which provides for personal information amendment[22].

Chapter 3 of the IP Act contains rights of access to, and amendment of, personal information in the possession or control of an agency. An agency is defined as including a Minister, department, local government or public authority. Chapter 2, part 4 cannot apply where the contracting entity is an agency[23] and, despite being bound to comply with the privacy principles, a bound contracted service

[20] Contractors to health agencies comply with the NPPs; contractors to all other agencies comply with the IPPs.
[21] IPP 6(2)(a); NPP 6(2)(a).
[22] IPP 7(2); NPP 7(2).
[23] Section 34(1) of the IP Act.

provider does not *become* an agency. An individual cannot apply under Chapter 3 of the IP Act to the bound contracted service provider to access or amend personal information.

If an individual tried to apply under Chapter 3 of the IP Act the bound contracted service provider would be entitled to refuse access or amendment. Because they are entitled to refuse to give access to, or amend, personal information under a State law they are also entitled to do so under IPPs 6-7 or NPPs 6-7.

It would arguably still remain open for a bound contracted service provider to give access to, or amend, personal information but it would be discretionary and not required. This could result in situations where the community is unable to:

- access their personal information when it is held by contracted service provider; or
- have incorrect personal information held by a contracted service provider amended.

If a bound contracted service provider is authorised by the privacy principles to refuse access or amendment a privacy complaint (the remedy for a failure to comply with the privacy principles) will not assist the individual.

It does not appear to OIC that it was intended that bound contracted service providers would be able to avoid access and amendment obligations in the IPPs and NPPs. OIC suggests that removing this impediment be investigated.

APPENDIX A: RELEVANT SECTIONS OF THE *INFORMATION PRIVACY ACT 2000* (VIC)

Information Privacy Principle 9-Transborder Data Flows

9.1. An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if-

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply-

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain that consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles.

Back to discussion of section 33.

Section 25 Complaints

(1) An individual in respect of whom personal information is, or has at any time been, held by an organisation may complain to the Privacy Commissioner about an act or practice that may be an interference with the privacy of the individual.

(2) A complaint may be made under subsection (1) if-

(a) there is no applicable code of practice in relation to the holding of the information by the organisation; or
(b) there is an applicable code of practice in relation to the holding of the information by the organisation but that code does not provide for the appointment of a code administrator to whom complaints may be made; or
(c) there is an applicable code of practice in relation to the holding of the information by the organisation that provides for the appointment of a code administrator and not less than 45 days before complaining under subsection (1) the individual complained to the code

administrator in accordance with the procedures set out in that code but has received no response or a response that the individual considers to be inadequate.

(3) In the case of an act or practice that may be an interference with the privacy of 2 or more individuals, any one of those individuals may make a complaint under subsection (1) on behalf of all of the individuals with their consent.

(4) A complaint must be in writing and lodged with the Privacy Commissioner by hand, facsimile or other electronic transmission or post.

(5) It is the duty of employees in the office of the Privacy Commissioner to provide appropriate assistance to an individual who wishes to make a complaint and requires assistance to formulate the complaint.

(6) The complaint must specify the respondent to the complaint.

(7) If the organisation represents the Crown, the State shall be the respondent.

(8) If the organisation does not represent the Crown and-

(a) is a legal person, the organisation shall be the respondent; or

(b) is an unincorporated body, the members of the committee of management of the organisation shall be the respondents.

(9) A failure to comply with subsection (6) does not render the complaint, or any step taken in relation to it, a nullity.

Section 29 Circumstances in which Privacy Commissioner may decline to entertain complaint

(1) The Privacy Commissioner may decline to entertain a complaint made under section 25(1) by notifying the complainant and the respondent in writing to that effect within 90 days after the day on which the complaint was lodged if the Privacy Commissioner considers that-

(a) the act or practice about which the complaint has been made is not an interference with the privacy of an individual; or
(b) the act or practice is subject to an applicable code of practice and all appropriate mechanisms for seeking redress available under that code have not been exhausted; or
(c) although a complaint has been made to the Privacy Commissioner about the act or practice, the complainant has not complained to the respondent; or
(d) the complaint to the Privacy Commissioner was made more than 45 days after the complainant became aware of the act or practice; or
(e) the complaint is frivolous, vexatious, misconceived or lacking in substance; or

(f) the act or practice is the subject of an application under another enactment and the subject matter of the complaint has been, or is being, dealt with adequately under that enactment; or

(g) the act or practice could be made the subject of an application under another enactment for a more appropriate remedy; or

(h) the complainant has complained to the respondent about the act or practice and either-

(i) the respondent has dealt, or is dealing, adequately with the complaint; or

(ii) the respondent has not yet had an adequate opportunity to deal with the complaint; or

(i) the complaint was made under section 27, on behalf of a child or a person with a disability, by an individual who has an insufficient interest in the subject matter of the complaint.

(2) A notice under subsection (1) must state that the complainant, by notice in writing given to the Privacy Commissioner, may require the Privacy Commissioner to refer the complaint to the Tribunal for hearing under Division 5.

(3) If the act or practice could be made the subject of an application under-

(a) the Privacy Act 1988 of the Commonwealth; or
(aa) the Disability Act 2006; or
(ab) Part VIA of the Freedom of Information Act 1982; or
(b) the Ombudsman Act 1973-

the Privacy Commissioner may refer the complaint to the Federal Privacy Commissioner, the Disability Services Commissioner, the Freedom of Information Commissioner or the Ombudsman, as the case may be, and notify the complainant and the respondent in writing of the referral.

(4) Before declining to entertain a complaint, the Privacy Commissioner may, by notice in writing, invite any person-

(a) to attend before the Privacy Commissioner, or an employee in the office of the Privacy Commissioner, for the purpose of discussing the subject matter of the complaint; or
(b) to produce any documents specified in the notice.

(5) Within 60 days after receiving the Privacy Commissioner's notice declining to entertain a complaint, the complainant, by notice in writing given to the Privacy Commissioner, may require him or her to refer the complaint to the Tribunal for hearing under Division 5.

(6) The Privacy Commissioner must comply with a notice under subsection (5).

(7) If the complainant does not notify the Privacy Commissioner under subsection (5), the Privacy Commissioner may dismiss the complaint.

(8) As soon as possible after a dismissal under subsection (7), the Privacy Commissioner must, by written notice, notify the complainant and the respondent of the dismissal.

(9) A complainant may take no further action under this Act in relation to the subject matter of a complaint dismissed under this section.

Back to discussion on complaints.