Applying the legislation

GUIDELINE *Information Privacy Act 2009*

Privacy myths—busted!

People commonly think privacy means no one can know anything about them, no one can gather information about them, and no one can use or pass on information about them. This is not correct. The reality is that the privacy principles in the *Information Privacy Act 2009* (IP Act) are about balance: allowing necessary information flow to enable the delivery of government services while protecting personal information from misuse or abuse.

It is a myth that privacy is absolute. In actuality, the privacy principles provide generous flexibilities in areas where common-sense would expect there to be a measure of relaxation – such as law enforcement and public safety. This guideline helps clear up some other common privacy myths.

Myth: If there's no name disclosed, there's no privacy breach

Not necessarily. Information with the name removed can still be personal information.

The IP Act defines personal information as information about an individual whose identity is apparent from the information or can 'reasonably be ascertained' from the information. Agencies should not assume that de-identification is a simple matter of removing an individual's name. Whether the identity of an individual can be worked out will depend on the type and detail of the initial information, and how easily this can be tied in with other known information.

Myth: Privacy makes dealing with an emergency harder

Not correct. The IP Act actually makes it easier to collect, use and share personal information in an emergency situation.

Effective information flow is critical in emergency situations, and the IP Act has special rules that can apply in an emergency: agencies do not need to give a collection notice when delivering an emergency service and can use or disclose information as needed to prevent or lessen a serious threat to an individual or to public safety.

Myth: Privacy stops government from using social networks

Not correct. Social networks can be an important part of an agency's communication strategy; privacy simply has to be part of that strategy. Agencies moving to a social network need:

- a clear and accessible policy about how it will use the personal information collected through the social network
- to secure the personal information it collects against unauthorised access or use

- to be careful when disclosing personal information or sending it overseas (for example, where the social network operates from outside Australia). Often, to be compliant with the IP Act, you will need to obtain the person's permission to post their personal information to the social media site; and
- to manage the content posted on a social network in accordance with the recordkeeping requirements of the *Public Records Act 2002*.

Myth: Privacy stops government from using cloud services

Not correct. A cloud service arrangement with robust security and accountability safeguards can not only be compatible with the IP Act, but may in fact enhance the protections for some government-held information.

While some cloud services operate from overseas, and the IP Act does have rules about overseas transfer, the rules are there to ensure that personal information leaving the country remains protected. This shouldn't create any problems, because Queensland government agency contracts for cloud services will, at their heart, be about ensuring the security and integrity of the service. A cloud services contract which robustly deals with the collection, storage, use and disclosure of information will go a long way towards satisfying the IP Act's overseas transfer rules.

Myth: Privacy stops government information flow – you can't tell anyone anything

Not correct. The privacy principles provide for fair handling of personal information; they accordingly allow for the appropriate flow of personal information within and between agencies.

Where an agency has collected personal information for a particular purpose, there are no restrictions on an agency using the personal information for that purpose. Where the individual was made aware that their information will be passed to a third party, the information can also be disclosed. There are a number of circumstances under which personal information obtained for one purpose can be used for a different purpose. There are similar circumstances for an agency providing personal information to third parties, including with the individual's express or implied consent.

Myth: Privacy and the *Right to Information Act 2009* contradict each other

Not correct. The IP Act and *Right to Information Act 2009* (**RTI Act**) work together to ensure an appropriate balance between privacy protection and government openness.

The IP Act allows people to access and amend their own personal information and protects personal information generally. The RTI Act encourages and supports the release of government information and allows people to apply for any information held by government. People can apply for information under the RTI Act and as long as doing so is not, on balance, contrary to the public interest, it will be released. Privacy is a significant public interest. In many cases—but not

all—releasing an individual's personal information to another person will be contrary to the public interest. Generally, the individuals involved will be consulted about any potential release.

Myth: Privacy doesn't apply to law enforcement

Not quite. The IP Act does apply to law enforcement agencies, but it has specific rules which sensibly ensure privacy does not hamper law enforcement activities. For example, covert surveillance could not work if an agency was required to tell an individual under surveillance that their personal information was being collected.

Where the law enforcement activity reasonably requires it, the IP Act allows certain privacy principles to be disregarded, and it allows for necessary use and disclosure of personal information. Also the privacy principles do not apply to certain law enforcement documents. Other activities of law enforcement agencies are still subject to the full obligations of the privacy principles, such as human resources activities.

Myth: The IP Act applies to material in the public domain

Not really. The IP Act has specific relaxations for personal information that is publicly available:

- you are not disclosing personal information if you give it to someone who already knows the information or is in a position to find it out; for example, if that information is publicly accessible;
- the privacy principles do not apply to generally available publications[1], for example, public registers, electoral rolls, telephone directories, or to Queensland Parliamentary proceedings or published decisions of courts and tribunals, but do apply to any action that an agency takes with the information contained in the publication; and
- personal information published by an individual loses some of the IP Act's privacy protections; any related or connected information is not subject to several privacy principles. Publishing includes radio, print and television media as well as posting on the internet.

Myth: Privacy means you have to get the individual's consent before dealing with their personal information

Not quite. Consent is one of a number of exemptions for the secondary use or disclosure, or transfer overseas, of personal information, but an agency is not obliged under the IP Act to pick consent over another exemption.

A common misconception is that an agency must obtain the consent of the individual before asking a third party for personal information about the individual. An agency also does not require the individual's consent to store their personal

[1] See schedule 1 (7)(a) of the IP Act.

information or to use it, however obtained, for the purpose for which it was collected.

Myth: If someone breaches an individual's privacy they can be fired or fined under the IP Act

Not correct. The IP Act allows individuals to make privacy complaints about a breach of their privacy.

The privacy complaint jurisdiction is remedial in nature. The IP Act does not provide for an agency to be fined or an employee to be fired for breaching an individual's privacy. In some circumstances, privacy complaints may be heard by the Queensland Civil and Administrative Tribunal (QCAT), but the orders QCAT can make are similarly focussed on remedying the breach, with no capacity to fine or otherwise penalise the agency.

QCAT can declare that a breach occurred, order an apology and order that no further breaches occur. It can also order the agency to compensate the individual for damages caused by the breach. The maximum it can award is $100,000; the individual has the onus of showing they have suffered the damage.

However, a breach of privacy by an agency officer could potentially also be a breach of the Public Service Code of Conduct or a breach of another Act applicable to that agency. In these cases, disciplinary actions taken under these parallel obligations could result in adverse consequences for the officer concerned.

For additional information and assistance please refer to the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or email enquiries@oic.qld.gov.au.

This guide is introductory only, and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

If you have any comments or suggestions on the content of this document, please submit them to feedback@oic.qld.gov.au.

Published 15 February 2013 and Last Updated 16 December 2015

Changes to legislation after the update date are not included in this document