A New Era of Privacy in Queensland

Julie Kinross
Information Commissioner
Office of the Information Commissioner Queensland

A NEW ERA OF PRIVACY IN QUEENSLAND

Julie Kinross, Office of the Information Commissioner (Qld)

July 2009 saw the introduction of Queensland's first information privacy legislation, the *Information Privacy Act 2009*. For the first time, all levels of Queensland government will be subject to privacy obligations: departments, public authorities and Ministers from 1 July 2009; local government from 1 July 2010.

Queensland's Information Privacy Act was part of the Right to Information reforms, which arose from an independent and comprehensive review of Queensland's freedom of information legislation. The review panel, chaired by Dr David Solomon AM, delivered The Right to Information Report in June 2008. It recommended the Government overhaul its approach to information. It proposed moving to a 'push' model, with greater proactive and routine release of information, new right to information and privacy legislation and maximum disclosure of non-personal information.

The goal of the push model was to make the Queensland government as open and accountable as possible.

The Information Privacy Act acts in concert with the *Right to Information Act 2009* to create a balance between maximum disclosure of government information and protection of an individual's personal information. It strives to ensure there are no arbitrary interferences with an individual's privacy and provides remedies should such arbitrary interference occur. Sometimes, in specific circumstances, individual privacy must give way to the legitimate needs of government; however these situations must be as open and accountable as the government itself. Open and accountable government must not come at the cost of individual privacy; there must be no arbitrary interference with that right.

HISTORY

Ultimately, the right to privacy is a human right. Article 12 of the Universal Declaration of Human Rights states:

No one shall be subjected to arbitrary interference with his privacy…everyone has the right to the protection of the law against such interference or attacks.

The path to Queensland's Information Privacy Act has been a long and winding one. 1971 saw the introduction of the *Invasion of Privacy Act 1971*, dealing with such matters as listening devices and invasion of home privacy. 1998 saw the tabling of the report *Privacy in Queensland* by the Legal, Constitutional and Administrative Review Committee.

2001 introduced two Information Standards – Information Standard 42, based on the Federal Privacy Act's Information Privacy Principles, and Information Standard 42A, applicable only to Queensland Health and based on the Federal Privacy Act's National Privacy Principles.

2003 was notable as it saw the District Court decision in *Grosse v Purvis* make Queensland the only jurisdiction in Australia to unequivocally recognise the existence of a tort of invasion of privacy, although it has yet to be canvassed in other Queensland decisions.

In 2005 sections 227A-227C were inserted into the Criminal Code to regulate 'observations or visual recordings in breach of privacy', creating a right to privacy which placed obligations not to interfere with that right on members of the public.

The Information Privacy Act stands on the shoulders of these forays into previous privacy protections, incorporating the lessons learned with best practice from other privacy jurisdictions to provide Queenslanders with a comprehensive and uniquely Queensland suite of privacy protections and remedies.

THE INFORMATION PRIVACY ACT

The objects of the Information Privacy Act are simple: government should provide people with the greatest level of access to, and amendment of, their personal information and the maximum protection of their personal information.

It achieves these objects in two ways: by providing a right of access and amendment in Chapter 3 of the Act and by obligating government in Chapter 2 to comply with the privacy principles when dealing with personal information.

Personal information

But what is personal information? It is the key to the Information Privacy Act, so it is important to understand exactly what it encompasses. Personal information is defined in the Act extremely broadly. It is any information or opinion about an individual. It need not be true and it need not be in a material form. The name of the individual does not have to be part of the information. As long as the individual can be reasonably identified, even if doing so requires reference to other information, it will be personal information. The main limitation on this is information about the deceased: this is not personal information, as the Queensland Acts Interpretation Act defines an individual as a natural person, which can only be a living individual.

Chapter 3

The right of access in Chapter 3 is subject to the public interest. If it would not be in the public interest, or in the interest of the individual requesting the information, for it to be disclosed then the government may withhold it. This could occur where, for example, release would endanger an ongoing investigation or reveal a confidential source of information, or where providing the information to the individual could have a detrimental effect on their mental or emotional well-being. Amendment is permitted where the personal information is inaccurate, out of date, incomplete or misleading. Even if the government decides this is not the case, and refuses to amend, the individual has the power to require a notation be added to the information, setting out their view of what the information should be.

In this way, Chapter 3 strikes a balance between the public interest and the interest of individuals in having control over, and knowledge about, their personal information held by government.

Chapter 2

Chapter 2 contains the obligations to comply with the privacy principles and sets out the situations in which the obligations need not be complied with.

The Act contains four sets of privacy principles:

- the Information Privacy Principles, or IPPs
- the National Privacy Principles, or NPPs
- the Transfer out of Australia principles, contained in section 33, and
- the Contracted Service Provider principles contained in Chapter 2, Part 4.

Which privacy principles apply depends on which government agency is being considered. Queensland Health is subject to the NPPs, due to its need to deal both with health information and other healthcare providers, while all other agencies are subject to the IPPs. The other privacy principles apply equally to all agencies.

What is the obligation?

An agency must not do anything which would result in a contravention of the privacy principles. An agency must not fail to do something where the failure would result in a contravention of the privacy principles.

What are the exceptions?

The Information Privacy Act protects the privacy of individuals, but it also recognises that there are times that privacy must give way to the greater public interest. As such, it provides some exceptions to the obligation to comply with the privacy principles. To ensure the interference with privacy is not arbitrary, each of the exceptions requires certain preconditions to be met before they can be relied upon.

Where an individual has published their personal information, or provided it to someone else for the purposes of publication, the agency need not comply with certain privacy principles. This is limited only to the personal information of that individual which is connected with or related to whatever personal information they published or provided for publication.

Where an agency provides information to its Minister or Ministers, it does not contravene the privacy principles, as long as the information is needed to inform the Minister of her or his portfolio responsibilities.

Law enforcement agencies, excluding Queensland Health, are permitted to be noncompliant with certain privacy principles, as long as the agency is satisfied on reasonable grounds that the noncompliance is necessary for its law enforcement functions. *Law enforcement agency* is defined broadly, and encompasses the Queensland Police Service, the Crime and Misconduct Commission and the Community Safety department, but it also encompasses any agency, or part of an agency, that has responsibility for the prevention, detection, investigation, prosecution or punishment of offences or breaches of the law attracting penalties or sanctions.

What do the privacy principles require?

The IPPs and the NPPs are similar in their requirements. Both create rules about collection, storage, accuracy, use and disclosure of personal information. These rules strike a balance between the individual right to privacy and the legitimate needs of government in service to the public interest.

Agencies may collect whatever personal information they legitimately need to carry out their functions, but that is all they may collect. They may not collect personal information *just in case*, on the off chance they might need it in the future. They must tell people why they want the information, any authorities under which it is collected, and anyone to whom it will be given. They must not interfere unreasonably with the private lives of individuals when collecting it, and they must not do so by unfair or illegal means.

Personal information is valuable, and its loss or unintended disclosure can have significant consequences for the individual. Agencies must protect the personal information they hold against loss, they must ensure that it is not accessed used, modified or disclosed without authority. They must ensure it is not misused and apply to it the appropriate levels of security.

Information privacy is at its heart about ensuring individuals are informed about their personal information and can access it is appropriately. To this end, government agencies must make people aware of the kinds of personal information they hold and how access to it may be gained.

Incorrect information can lead to incorrect actions and unintended consequences. Incorrect *personal* information can have a significant negative impact on the individual. Agencies must take all reasonable steps to ensure information is accurate, up to date and complete before they use it.

Personal information can only be used to fulfil the purposes for which it was collected, and may only be disclosed to the individual it is about. These are the general rules that govern agency use and disclosure of personal information, but these general rules must have exceptions if government is to function, and so there are public interest exceptions to the general rules. If an individual agrees, if another law authorises or requires it, or if it is necessary for law enforcement or to prevent a serious threats to an individual or to the public, an agency may use or disclose personal information. If the personal information could contribute to research in the public interest which will not disclose identifying information, an agency may use or disclose it, subject to certain safeguards.

In addition to these obligations are the rules about sending personal information out of the country. Once beyond Australia's borders, personal information become more difficult to protect. In recognition of this fact, it may only be sent overseas if certain rules are met. It may be transferred out of the country if, for example, the individual agrees, if another law authorises or requires the transfer, or if the transfer is necessary to prevent a serious threat to an individual or to the public.

Contractors are becoming ever more prevalent in the business of government, with some government functions and activities being outsourced where to do so will better serve the public. Where this outsourcing involves the flow of personal information between government and contractor, the agency must take reasonable steps to bind the contractor to the Act as if it were an agency. If it dos so, the privacy principles will apply to the contractor, and the consequences of noncompliance will be the same for the contractor as they would be for the agency.

This is particularly important in light of the fact that a contractor who would otherwise be subject to the Federal Privacy Act is exempt from the privacy obligations in that Act when contracting with the Queensland government. A failure to take those reasonable steps could result in personal information being provided to a contractor who would have no obligations to appropriately protect it.

THE ROLE OF THE OFFICE OF THE INFORMATION COMMISSIONER

The Information Privacy Act places obligations on agencies to comply with the privacy principles, but it does not expect them to do this without assistance.

The Office of the Information Commissioner is responsible for providing information and assistance to Queensland government agencies (such as state government departments, local councils and universities), Ministers and the community to support agencies to comply with these laws; and for monitoring and reporting on the performance of government agencies.

The Office is Queensland's independent body established to promote access to government-held information and to protect people's personal information held by government. The Office also reviews specific agency decisions under these laws regarding access and amendment applications, deals with privacy complaints and makes certain decisions, including whether an agency's privacy obligations can be waived or modified in the public interest.

PRIVACY COMPLAINTS

One of the Office's most significant roles under the *Information Privacy Act 2009* is to conciliate privacy complaints. Under the Act, any individual who believes that an agency has dealt with their personal information in a way inconsistent with the privacy principles may make a complaint to that agency. The act or practice complained about must have occurred after 1 December 2009 for Ministers, departments and public authorities, and after 1 July 2010 for local government. An agency is allowed a minimum of 45 business days to deal with the complaint, at the end of which, if the individual has received no response or is dissatisfied with what they received, it may be brought to the Office.

It is important to understand that, beyond establishing jurisdiction and extending the 45 business day time limit for agencies, the Office does not have a decision making role with regard to privacy complaints. The Office's role is one of conciliation, to attempt to find a common ground between the agency and the individual, so that complaint may be resolved to the satisfaction of both, or at least to the dissatisfaction of neither.

Should conciliation be successful, the parties may register a certified agreement with the Queensland Civil and Administrative Tribunal, giving their conciliated outcome the force of an order of the tribunal. Should conciliation be unsuccessful, the individual who lodged the complaint may require the Information Commissioner to refer it to QCAT. QCAT is given a wide range of orders it may make, but the one that catches the attention immediately is the possibility of a compensation order of up to $100, 000.00

ISSUES OF INTEREST

To date, the Office has received very few privacy complaints, but the number has begun increasing. In the absence of privacy complaints, the privacy team has been busy addressing issues which are impacting on agencies as they come to grip with the new legislation.

Two issues of interest which have arisen several times are the question of positive disclosure and issues with personal information and the World Wide Web.

Positive disclosure describes a situation where an agency wishes to disclose personal information, and seeks to justify it by arguing that the disclosure would be 'good for the individual' or would show them in a positive light. It is a simple issue, but one that has been raised several times from different sources. The reality is that the privacy principles do not distinguish between 'bad' disclosure and 'good' disclosure. Anything that puts the personal information outside the control of the agency is a disclosure, and it must be justified under the privacy principles. The exceptions to the non-disclosure rule encompass situations of benefit to the public interest, not potential positive outcomes for the individual. If an agency believes that a disclosure will benefit an individual, then the simplest action is to ask the individual if they agree to their information being disclosed.

Often the way that agencies wish to make these positive disclosures is through their website, which leads into an entirely new issue.

Section 33 limits the situations in which personal information can be sent out of the country, which can raise issues with the use of the World Wide Web. The act of making personal information available on an agency webpage means that the information may be transferred out of Australia—all it takes is someone from another country to access it. A number of agencies have created Facebook accounts, many of which contain photographs of identifiable individuals. The act of uploading a photograph, or any personal information, to Facebook transfers it out of the country. Entities such as Google and the Internet Archive ensure that any personal information placed online is preserved, and as they cache copies of websites, they store the information on servers in America. Free web-based social networking and survey tools, such as YouTube or Survey Monkey, raise section 33 issues which must be addressed before an agency transfers personal information to them or uses them to collect personal information.

It is an increasingly prominent problem on which the Office has provided guidance in response to individual queries and in its information sheets and guidelines. As government moves to embrace Web 2.0, this issue is likely to arise even more frequently.

THE FUTURE

This is a challenging time for privacy. The Australian Law Reform Commission handed down its report and recommendations for the future of privacy in Australia, and the Federal government has responded. The Healthcare Identifiers Bill 2010 has been tabled in Federal Parliament and promises to change forever the way in which we relate our identity to our healthcare providers, and it is only the beginning of the future of e-Health in Australia. Our own Law, Justice and Safety Committee handed down its final report into Alcohol-related violence just this month, and its recommendations embrace increased CCTV, increased ID scanning, and the offering of incentives for the introduction of same.

We live in an information age that is casually miraculous and the blistering speed of technological change has dragged communication in its wake. The hand-written letter has progressed to e-mail to text messaging to inscribing messages on a Facebook Wall for all the world to see. Personal information was once housed in massive ledgers, recorded with the elegant swirl of a fountain pen; now it is electronic impulses and bits and bytes, a million ledgers in the palm of your hand.

In the face of this challenge and change, it is more important than ever that the people of Queensland have their right to privacy under an accountable government defined and enforced. The Information Privacy Act will prove a stalwart guardian of Queenslanders' privacy as we move forward into the future, and the Office of the Information Commissioner will support both government and the public in its application.