CLIFFORD
CHANCE

Briefing note May 2015

Is your organisation thinking about 'Privacy Everyday'?

When was the last time your organisation thought about privacy?

One of the key messages coming out of Privacy Awareness Week (held from 3 May 2015), an initiative of the Asia Pacific Privacy Authorities forum, is that organisations should be considering privacy every day. This central theme of 'Privacy everyday' has driven a discussion around embedding privacy in business culture, technology and infrastructure and products.

The Australian regulator, the Office of the Australian Information Commissioner (**OAIC**), has encouraged organisations to adopt 'privacy by design' practices, where privacy (and the overlapping issues of data protection and cyber security) should be considered at the beginning of all product development, from end user products to services which enhance product delivery.

To coincide with Privacy Awareness Week, the OAIC has released regulatory guidance as well as other resources to assist organisations with their compliance obligations.

Some of the notable publications released by the OAIC are discussed below.

Privacy Management Framework

Under Australian Privacy Principle (**APP**) 1.2 an organisation is required to put in place practices, procedures and systems to ensure compliance with the APPs. As the OAIC considers APP 1 a bedrock principle of APP compliance, it is important for organisations to use this as the foundation for how they approach privacy. The Privacy Management Framework, released on 4 May 2015, sets out steps to assist organisations in complying with APP 1.2.

The Framework is made up of four steps:

1. **Embed** a culture of privacy that enables compliance

   Personal information is to be treated as a valuable business asset which must be respected, managed and protected through a 'privacy by design' approach.

2. **Establish** robust and effective privacy practices, procedures and systems

   Policies and processes are important compliance tools which must be clear, up-to-date and effective for all stages of the information lifecycle, from collection through to use, disclosure and destruction once personal information is no longer required. Data breach response plans should be developed to provide guidance to the organisation in the event of a breach.

3. **Evaluate** privacy practices to ensure continued effectiveness

   As internal and external threats constantly change, so too must privacy practices. They cannot be static and must be constantly monitored and reviewed. Performance must be measured against an organisation's privacy management plan and employees and customers should be provided with channels to give feedback.

4. **Enhance** your response to privacy issues

   Organisations must constantly enhance their processes, particularly by using step 3 evaluations. An organisation may consider having their privacy processes externally assessed to ensure they incorporate new issues, trends and changing technology.

It's nothing personal: Privacy Commissioner's determination on 'personal information'

There has been limited guidance on what is covered by the term 'personal information' under the *Privacy Act 1988* (Cth) ("**Privacy Act**"). However, some guidance has been recently provided in a determination on 1 May 2015 by the Commissioner that metadata can be personal information. The determination was made in response to a complaint lodged by a journalist in 2013 that Telstra had breached his privacy by refusing him access to metadata relating to his mobile phone service.

Whilst the Commissioner's determination considered the definition of personal information prior to the 2013 Privacy Act reforms, which was narrower than the current definition, the determination does indicate a broad approach to 'personal information'. Relevantly metadata can be personal information, depending on the resources and capacities of the entity holding the metadata.

The Commissioner took the view that whilst extracting metadata would take time and the expertise of specifically qualified personnel, these considerations had little weight as Telstra had developed the capacity to inquire and cross-match metadata to ascertain a customer's identity for internal network assurance purposes and to accommodate requests for metadata from law enforcement agencies. The Commissioner determined that the metadata sought was personal information in the circumstances.

The Privacy Act

The Privacy Act currently defines 'personal information' as being:

- information or an opinion about an identified individual, or an individual who is reasonably identifiable:
  1. whether the information or opinion is true or not; and
  2. whether the information or opinion is recorded in a material form or not.

However, the determination does not appear consistent with the OAIC's Guidelines to the APPs which indicate that an individual will not be reasonably identifiable if the steps required to identify them are excessively time-consuming or costly. Telstra has indicated that it will appeal the determination.

Privacy Business Resource: Sending personal information overseas (APP 8)

APP 8 sets out onerous obligations for organisations with respect to cross-border disclosure of personal information. Its application in practice has been unclear. As a supplement to the OAIC's APP Guidelines, the OAIC has released a business resource which provides organisations with additional guidance on complying with APP8.

An organisation's APP obligations when they send personal information overseas will depend on whether there is a 'use' or 'disclosure' of information. A 'use' occurs where the organisation sends the information overseas but handles and manages information within their effective control. A 'disclosure' occurs where personal information becomes accessible to others outside the organisation and is no longer in the organisation's effective control.

The OAIC has recognised that in some instances it is difficult to determine whether the information is being 'used' or 'disclosed'. In both scenarios, the organisation is similarly accountable for the mishandling of that information by the recipient and the OAIC has stated that "where it is unclear whether the personal information is being used or disclosed, the best approach is to take reasonable steps to ensure the APPs are complied with" by the overseas recipient.

In relation to disclosure specifically, APP 8.1 provides that before personal information is disclosed overseas, an organisation must take reasonable steps to ensure that the recipient does not breach the APPs. The OAIC expects that APP entities will enter into enforceable contractual arrangements with overseas recipients to ensure compliance, which includes ensuring that such arrangements specify:

- the purpose(s) for which the overseas recipient may use or disclose personal information,
- minimum technical and organisational measures to be taken to ensure security of personal information overseas,
- agreed procedures for providing access to personal information on request; and
- mechanisms that enable the organisation to monitor compliance.

The OAIC recognises that negotiating such contractual arrangements can be a commercial challenge given that in many instances, overseas recipients may not want to be subject to Australian privacy obligations. Nevertheless the OAIC has made clear that the inability to ensure overseas recipients comply with the APPs could and should result in information not being sent to such recipients.

Consultation on the Guide to privacy regulatory action

On 5 May 2015 the OAIC released for public comment exposure drafts of three chapters of the Guide to privacy regulatory action, which provides an explanation of how the Commissioner will exercise his or her regulatory powers. The draft chapters address the following areas:

- the privacy complaint handling process,
- Commissioner determinations; and
- injunctions sought by the Commissioner.

Privacy Complaint Handling Process

The OAIC provides a free, informal and accessible complaint process to the public. In general, the OAIC will seek to resolve complaints through conciliation or, if conciliation does not resolve the matter, the Commissioner may make a determination of the complaint. When seeking to conciliate or determine a complaint, the OAIC has powers to investigate.

If jurisdiction to investigate has been established the OAIC will generally notify the relevant parties of the complaint and, to assist with resolving the complaint, any substantive information provided by a party to the complaint will be made available to other parties. This process means that the OAIC will generally not accept confidential submissions and will ask for information in a form that may be provided to the other party.

Commissioner Determinations

After investigating a complaint, the Commissioner has the power to make a determination which either dismisses the complaint or finds that the complaint is substantiated. Factors that weigh in favour of the Commissioner making a determination include that:

- there is a prima facie interference with privacy that cannot be resolved otherwise,
- one or both parties have requested resolution by determination,
- the issues are complex and/or systemic; and
- the investigation process has not been able to resolve whether an interference with privacy has occurred, and it is likely the determination process will resolve that question.

In investigations instigated by the Commissioner on his or her own initiative, consideration will be given to whether:

- the respondent has not co-operated and the Commissioner believes it necessary to make formally binding declarations; and
- there is a public interest in the Commissioner making a declaration setting out reasons for finding an interference with privacy has occurred.

Where the Commissioner makes a declaration that the complainant is entitled to compensation, it is guided by the following principles:

- awards should be restrained but not minimal,
- aggravated damages may be awarded in appropriate cases,
- compensation should be assessed having regard to the complainants reaction not the perceived reaction of the community or reasonable person; and
- once loss is proved, there needs to be a good reason as to why compensation should not be awarded.

In November 2014 the OAIC released a draft chapter of the Guide to privacy regulatory action which dealt with civil penalties under the Privacy Act, which can be sought for cases of serious or repeated interference with privacy by an organisation. The guidance provided that civil penalties are unlikely to be sought for minor or inadvertent contraventions, where the organisation responsible for the contravention has co-operated with the investigation and has taken steps to avoid future contraventions.

Injunctions

The Commissioner has the power to seek an injunction to prevent contravention of the Privacy Act. Such relief may be appropriate where conduct:

- is serious or has had, or is likely to have, serious adverse consequences,
- is systemic and poses ongoing compliance or enforcement issues,
- is deliberate or reckless or the entity involved is not cooperative; and
- raises significant concerns of public interest.

When considering whether to grant an injunction to restrain a person from engaging in conduct, the Court must be satisfied that:

- conduct in contravention of the Privacy Act has been engaged in; and
- if the injunction is not granted then the person will likely engaged in conduct in contravention of the Privacy Act

The court, in restraining a person from engaging in conduct, may also order that a person do any act or thing if it is in the Court's opinion desirable to do so, for example putting into place specified risk management practices to prevent future similar breaches of privacy.

What's next?

The OAIC has taken the opportunity of Privacy Awareness Week to highlight its priorities for 2015. The 'Privacy everyday' and 'privacy by design' approaches can be seen in guidance on APP 1 and 8 and how the Commissioner intends to exercise its regulatory power. With the advent of the metadata retention scheme, which will require telcos and internet service providers to store customers' metadata (such as the time and participants in phone calls, text messages and emails) for two years, and the overlap with personal information, the importance of ensuring privacy practices are embedded into everyday business processes will only continue to grow.

Contacts

Diana Chang
Partner
T: +61 28922 8003
E: diana.chang@cliffordchance.com

Timothy Grave
Partner
T: +61 2 8922 8028
E: Timothy.grave@cliffordchance.com

Jerrem Ng
Senior Associate
T: +61 2 8922 8069
E: Jerrem.ng@cliffordchance.com

Hong-Viet Nguyen
Senior Associate
T: +61 2 8922 8045
E: hong-viet.nguyen@cliffordchance.com