Privacy Act Amendments: What's the Impact for Information Security?

In May 2012, as part of Privacy Awareness Week, the Attorney General announced amendments to the Privacy Act 1988 (Cth), with the Amendment Bill (all 266 pages of it) introduced to Parliament in late May.[1] It is expected to pass through both Houses without issue.

The bill proposes a single set of privacy principles to apply to both Commonwealth agencies and private sector organisations, new credit reporting provisions, privacy codes, and increased powers and functions for the Privacy Commissioner to assist in resolving complaints, conducting investigations and promoting privacy compliance.

According to the Attorney[2] the key changes to benefit consumers are:

- clearer and tighter regulation of the use of personal information for direct marketing
- extending privacy protections to unsolicited information
- making it easier for consumers to access and correct information held about them
- tightening the rules on sending personal information outside Australia
- enhancing the powers of the Privacy Commissioner to improve the Commissioner's ability to resolve complaints, conduct investigations and promote privacy compliance

The proposed changes "represent the culmination of an extensive consultation process and will implement the Government's response to the Australian Law Reform Commission's report – For your information: Australian Privacy Law and Practice."[3] It does however only deal with the 197 recommendations considered by the Government in its first stage response to the 295 recommendations made by the Australian Law Reform Commission in its 2008 report. Nearly four years later, there is still no formal Government response to some important issues raised by that report – including removal of exemptions for smaller business, media organisations in the conduct of journalism and political parties, serious data breach

[1] The Bill is titled *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*. Gilbert and Tobin have very helpfully prepared an updated version of the *Privacy Act*, incorporating the proposed amendments – which is available **here**.

[2] From the Attorney General's Media Release "Privacy Laws Set to Reform: May 2, 2012 http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Second%20Quarter/2-May-2012---Privacy-laws-set-to-reform.aspx

[3] From the Attorney General's Media Release "Privacy Laws Set to Reform: May 2, 2012 http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Second%20Quarter/2-May-2012---Privacy-laws-set-to-reform.aspx

notifications and a statutory cause of action for serious invasion of privacy. Privacy law reform still has a long way to go.[4]

The Proposed Amendments

This paper will only look at those amendments most relevant to information security professionals including:

- The new privacy principles
- Increased powers to the Commissioner
- Changes to liability on the cross border transfer of data
- New Civil penalty regime.

Amendments to the credit reporting provider provisions and requirements in relation to privacy notices and the obtaining of consent may also be of interest – but are not covered here.

Australian Privacy Principles (APPs) – Data Security Principle

The National Privacy Principles for the private sector and Information Privacy Principles for the public sector, will be repealed and replaced by a single set of 13 Australian Privacy Principles (APPs) that will be applicable to both Commonwealth agencies and private sector organisations (known as APP entities). Under the new APPs there is no substantive change to the previous Data Security Principle requiring all organisations to take reasonable measures to secure personal information from unauthorised access, loss or disclosure.

Privacy Commissioner's Functions and Powers

The Bill's provisions will clarify the Commissioner's functions and grant new powers, aligning the Privacy Commissioner more closely with those of his regulatory counterparts (such as ASIC and the ACCC).

The current functions of the Commissioner can be categorised as follows:

- **guidance-related** - including publishing guidelines, promotion and education;
- **monitoring-relating** - including monitoring security and accuracy, evaluating compliance, and examining proposed enactments for potential privacy impact; and
- **advice-related** – including advising and reporting to the Minister on matters relating to the Privacy Act, informing the Minister of the actions a Commonwealth agency needs to take to comply with the Australian Privacy Principles (APPs).

The Bill's amendments will allow the Commissioner to:

- "**Own motion" investigations:** on its own motion, investigate any act or practice which may be an interference with an individual's privacy (being a breach of an APP or a registered APP code binding on the entity) and which the Commissioner considers desirable to investigate – and to make a determination as a result of an on

[4] http://foi-privacy.blogspot.de/2012/05/privacy-law-reform-stage-1-in.html

motion investigation. The existing Act does not allow the Commissioner to take any particular action following the conclusion of an OMI. Under the amendments, actions now available to the Commissioner following an OMI include:

- making a declaration that an interference of privacy has occurred;
- ordering an entity to take specific actions to prevent further repeats of the acts or practices investigated;
- ordering an entity to redress or compensate any loss or damage suffered (loss or damage may include humiliation suffered by the complainant or injury to the complainant's feelings); and
- making any order the Commissioner considers appropriate.

In support of these new powers, the Commissioner will also have the right to commence proceedings in the Federal Court or the Federal Magistrates Court to enforce such determinations.

These new powers are of significance to information security practitioners as all of the last 5 OMI's by the Privacy Commissioner have included consideration of breaches of the Data Security Principle. As well, the Commissioner has indicated an increased preparedness to use his OMI powers in the case of data breaches – particularly where there has been no prior voluntary notification to the Office of the breach.

The Privacy Commissioner believes that these powers give him the right, for instance to require the application of security patches or the adoption of a stronger security system.[5]

- **Compliance assessment**: conduct an assessment of whether an entity's handling of personal information complies with the APPs.
- **Enforceable undertakings:** accept enforceable undertakings from an entity to take certain actions or to refrain from taking certain actions. The Commissioner may apply to the Federal Court or the Federal Magistrates Court to compel an entity to comply with an undertaking or to pay compensation for any loss or damage caused by non-compliance with an undertaking;

Other news powers include;

- **privacy impact assessments:** direct a Commonwealth agency to conduct a privacy impact assessment of any proposed activity which could have impact on privacy;
- **conciliation:** conciliate complaints lodged with the Commissioner.

[5] Darren Pauli "Proposed reforms could mandate patching, security upgrades" May 23, 2012 http://www.scmagazine.com.au/News/301933,aussie-biz-face-11-million-for-repeat-breaches.aspx?eid=7&edate=20120523&utm_source=20120523&utm_medium=newsletter&utm_campaign=daily_newsletter

The APF says "the improvements concerning the Privacy Commissioner are of little use unless complainants can require that the Commissioner make formal decisions under s52 of the Act. The Commissioner has made one s52 decision in 6 years, and says complainants have no right to formal decisions. Government proposals to allow such complainants to go direct to the Federal Court have been dropped."

Cross Border Data Disclosures

With regard to cross-border disclosures an organisation will need to include in the privacy policy statement whether it is likely to disclose an individuals' personal information to overseas recipients, and if so, the countries in which such recipients are likely to be located. Freehills outlines other aspects of these changes.[6]

Under the proposed APP 8.1, an entity that discloses personal information to a recipient outside of Australia will be required to take 'such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs'. The government has indicated that in practice this will often involve entering into a contractual relationship with the overseas recipient

Australian entities that disclose personal information to overseas recipients will generally be liable for privacy breaches committed by those recipients (although they should also have contractual recourse against the recipient). This reflects a shift away from the 'adequacy approach' seen in NPP 9 and the EU to an 'accountability approach', as adopted by APEC and Canada. There will be some exceptions to the 'reasonable steps' and accountability obligations. One of these is where the recipient is subject to a law or binding scheme similar to the APPs which give appropriate enforcement rights to the individuals. Guidance from the OAIC is anticipated on this point. Notably, contractual provisions will no longer be sufficient alone to avoid accountability. Consent will also provide an exception, but must be more explicit than under NPP 9.

It should be noted that APP 8 is not intended to apply 'where personal information is routed through servers that may be outside Australia.' Entities will however need to take reasonable steps to ensure that personal information routed outside Australia is not accessed by overseas recipients as this will be considered disclosure."

[6] http://www.freehills.com/8113.aspx?source=rss#page=1

The APF says these changes mean "personal information of any Australians can now be sent to countries with no privacy laws at all, with victims required to prove breaches occurring there."

Civil penalty regime

The Bill also introduces into the Act for the first time a civil penalties regime.

Certain provisions in the Act will be designated as civil penalty provisions. Where a direct or ancillary contravention of a civil penalty provision has occurred, the Commissioner will be able to apply to the Federal Court or the Federal Magistrates Court for a civil penalty order.

Such provisions are mainly concerned with credit reporting, but a serious or repeated interference with the privacy of individuals (ie. a breach of an APP or a registered APP Code binding on the entity) will now carry civil penalty provisions.

Under the Bill, civil penalties range from 200 penalty units—$22,000 for an individual and $110,000 for a company—to 2,000 penalty units, which is $220,000 for an individual and $1.1 million for a company. For serious and repeated breaches of privacy, the penalty will be 2,000 penalty units.

Delayed Commencement

The majority of the new provisions hav0e a deferred commencement of nine months from the day after the Bill receives Royal Assent, in order to allow organisations and agencies time to prepare for the introduction of the new provisions.will come into effect nine months after assent.

Conclusion

The amendments address one of the biggest issues in regard to the Commissioner's OMI powers by granting extensive rights to make orders, which will be judicially enforceable. Although questions remain as to the willingness of the Privacy Commissioner to make determinations- given that he has had that power since 2001 and has made only 1 determination since 2004 - from an information security practitioners point of view the increased powers to make orders and the new civil penalty regime mean that even greater attention should be paid to ensuring that reasonable security measures are applied to all personal data.

References:

FOI Privacy Blogspot : http://foi-privacy.blogspot.de/2012/05/privacy-law-reform-stage-1-in.html

http://www.computerworld.com.au/article/425389/privacy_act_changes_finally_introduced_parliament/

http://www.theaustralian.com.au/national-affairs/laws-weaken-privacy-protection/story-fn59niix-1226365013213

http://www.ag.gov.au/Privacy/Pages/Privacy-Reforms.aspx

http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Second%20Quarter/2-May-2012---Privacy-laws-set-to-reform.aspx

Law Firm Commentary:

Freehills http://www.freehills.com/8113.aspx?source=rss#page=1

Mallesons http://www.mallesons.com//publications/marketAlerts/2012/Pages/Privacy-Amendment-Enhancing-Privacy-Protection-Bill-2012-introduced-into-Parliament.aspx#page=1

Minter Ellison http://www.minterellison.com/Publications/Privacy-Amendment-Bill/?utm_source=privacy%20amendment%20bill&utm_medium=email&utm_campaign=alert#page=1

Clauton Utz - here and here
http://www.claytonutz.com/publications/edition/7_june_2012/20120607/revamped_privacy_act_gives_the_privacy_commissioner_more_bite.page

http://www.claytonutz.com/publications/edition/24_may_2012/20120524/introduction_of_privacy_bill_to_parliament.page#page=1

Gibert and Tobin
http://ecomms.gtlaw.com.au/rv/ff00063ddcb7126ea13d1a55a24c84ab3388efed#page=1