Privacy enforcement in Australia is strengthened: gaps remain

Civil penalties exceeding 1 million Euros are possible, but gaps remain in appeals and transparency

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

(2014) 128 *Privacy Laws & Business International Report* 1-5

Australia's *Privacy Act 1988* now includes considerably stronger enforcement powers, including civil penalties of up to AUD$1.7 million (1.15 million euros), in effect from 12 March 2014. This article first outlines the new powers, deficiencies in appeal rights and transparency which may reduce their effectiveness, and the Commissioner's draft 'enforcement policy'. Two further developments remain unresolved: mandatory data breach notification (MDBN); and a statutory 'privacy tort'.

The 2014 reforms are a result of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* ('the Amendments'). It also amended the Privacy Act by including a new set of thirteen Australian Privacy Principles (APPs) to replace the National Privacy Principles (NPPs) previously applying to the those parts of the private sector covered by the Act, and the Information Privacy Principles (IPPs) applying to the federal public sector. There is little innovative about the APPs, and in some respects they will weaken the NPPs and IPPs.[1] None of the thirteen APPs is, overall, an improvement, and eight are worse for privacy protection.[2] The new data export provision will in some cases require more disclosure by companies. The APPs are not discussed further here.

New enforcement powers

The new enforcement powers only operate within the limited scope of the *Privacy Act 1988*. The Act still exclude from their operation employment records, political parties and so-called 'small' businesses, even though the Australian Law Reform Commission recommended the removal of these exclusions in its 2008 Report. 'Small' businesses are those with an annual turnover under AUD$3 million, and it has been estimated that they account for over 90% of all Australian businesses. No such exemptions are found in the EU Directive, and they help explain why

[1] For analysis, see Graham Greenleaf and Nigel Waters 'Australian Privacy Principles – Two Steps Backwards' (2010) 106 *Privacy Laws & Business International Newsletter*, pgs. 13-15. For more detail, see Graham Greenleaf and Nigel Waters (for Australian Privacy Foundation) 'A Critique of Australia's Proposed Privacy Amendment (Enhancing Privacy Protection) Bill 2012' (SSRN, 2012) < http://ssrn.com/abstract=2134838>

[2] The weaknesses of the APPs from a consumer perspective are summarised in Graham Greenleaf and Nigel Waters 'Australia's Privacy Bill 2012: Weaker principles, stronger enforcement' (2012) 118 *Privacy Laws & Business International Report*, pgs 16-18, July 2012, as follows: 'APP 1 (Openness) fails to require disclosure of the destination and recipients of personal information sent overseas. APP 2 (Anonymity and pseudonymity) destroys the existing right to anonymous transactions. APP 3 (Collecting solicited information) abandons existing limitations on collection and adds a raft of new exemptions. APP 5 (Notification of collection) does have improvements, but they are insufficient, particularly the failure to require disclosure of overseas recipients (now needed because of the weakness of APP 8). APP 6 (Use and disclosure) has the same raft of new exceptions as APP3, and is also worse than the existing principles in that it excludes the operation of the direct marketing and identifier principles. APP 7 (Direct Marketing) should apply to direct marketing by government as well. The consumer's right to ask 'Where did you get my name?' can be avoided wherever it is 'impracticable' for a business to do provide an answer. APP 8 (Cross-border disclosure) The 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. The weak disclosure requirements in APP 1 and APP 5 make this even more dangerous. The existing inadequate principle (NPP 9) needed strengthening, but it has been made worse. APP 9 (Government identifiers) removes protection against private sector misuse of government identifiers. APP 4 (Receiving unsolicited information), APP 10 (Quality), APP 11 (Security and deletion), APP 12 (Access), and APP 13 (Correction) are no worse than the existing principles, but no better.'

Australia's laws are not considered 'adequate' by the EU, unlike those of neighbouring New Zealand.

Seven changes to the enforcement aspects of the Act are important.

1. **Civil penalty provisions for 'serious' or 'repeated' breaches** A new civil penalty provision is satisfied where an act or practice of any entity covered by the Act is a 'serious interference' with a person's privacy, or the entity 'repeatedly' does an act which is an interference with the privacy of one or more persons (s13G). What makes a breach 'serious' is not defined, and 'repeatedly' is also undefined. For a civil penalty to be applied, the Commissioner must apply to the Federal Court or Federal Magistrates Court (s80W). The civil penalty is determined by the court, to the maximum of up to AUD$1.7 million (1.15 million euros) for companies, or up to AUD$340,000 (230,000 euros) for individuals.[3] In determining the amount of civil penalty, the court may consider all relevant matters including any loss or damage resulting from the breaches. The penalty is paid to the government, but the Commissioner could also award compensation to a complainant in relation to the same breaches of the Act under section 52. The new Part VIB ('Civil Penalty Orders') only applies to breaches of section 13G and some credit reporting breaches, but could easily be applied in future to new categories of breaches.

2. **Power to make determinations following 'Commissoner initiated' investigations** The Commissioner has always been able to investigate on his own initiative (or 'own motion') acts or practices that might be an interference with privacy (s40(2)). He or she is now newly empowered to make a 'determination' (formal order) after such a 'Commissioner initiated' investigation (s52(1A)). Such a determination can include orders prohibiting continuation of the act or practice, requirements to take steps to ensure that acts or practices cease, requirements to take specified remedial actions, and declarations that one or more individuals are entitled to compensatory damages. These are substantial powers.

3. **Commissioner can accept enforceable undertakings** The power to accept enforceable undertakings from entities (s33E) should be a significant enhancement of the Commissioner's ability to settle investigations without formal orders but with enforcement. It does not require a prior finding of an 'interference with privacy' (ie a breach of the Act) before an undertaking may be accepted. It applies to both complaint investigations and Commissioner-initiated investigations. If such an undertaking is breached, the Commissioner may apply to the Federal Court or Federal Magistrates Court to enforce it, and the court may also order compensation to persons affected by the breach of the undertaking, or make any other appropriate orders (s33F). It appears that undertakings can be directed at ensuring that future acts or practices will not interfere with the privacy of individuals generally (s33E(1)(c)), not only a specific complainant, so it has broad potential for the Commissioner to provide directions in areas of likely privacy invasion. The value of transparency is enhanced by the fact that the Commissioner 'may publish the undertaking on the Commissioner's website' (s33E(5)), but this is not compulsory. Some undertakings may need to be anonymised, either to protect the privacy of a complainant, or where necessary for a settlement. Whether the Commissioner will routinely publish undertakings (either identified or anonymised) is not known.

4. **Broader orders possible after complaint determinations** The Act now allows the Commissioner to make 'any order that the Commissioner considers necessary or appropriate' (s52(1)(ia)), including orders directing respondents to take specific actions to

[3] For section 13G, 2,000 penalty units (for individuals), or up to five time that for a corporate defendant.

remedy a complaint. There was previously some doubt about whether the Commissioner could order *how* a breach of the Act must be remedied. Australia's legislation has always allowed the Commissioner to make orders for the payment of compensation by a s52 determination. It is the only privacy legislation in the Asia-Pacific giving a data protection authority such a power, and unusual globally. However, compensation has only been ordered on three occasions.

5. **Right of appeal to the AAT** The amended Act will give dissatisfied complainants and respondents a right of appeal. For the first time in 25 years[4] they can appeal to the Administrative Appeals Tribunal, against the Commissioner's formal decisions under section 52 on the merits of their complaint (s96(1)(c)). It is a long overdue reform, but as explained in the next section, may mean nothing.

6. **Compliance 'assessments' of any public or private sector organisation** The Commissioner can now conduct 'assessments' of the compliance of any public or private sector organisation (all 'APP entities') with the APPs or other enforceable privacy obligations (s33C). This replaces the audit function of the Commissioner, which did not apply to companies' compliance with the NPPs. It is not clear if this effectively extends full audit powers to all private sector organisations covered by the APPs, as recommended by the ALRC.[5]

7. **Privacy Impact Assessments (PIAs) by agencies** New powers to the Commissioner to require Privacy Impact Assessments (PIAs) from federal government agencies (s33D)) are desirable. However, they are defective in not requiring PIAs to be either independent or public. Many PIAs have apparently been conducted in Australia, but few have been made public to assist in public debate on important initiatives. Unfortunately, there is no provision to ensure that requested PIAs are completed before decisions are made to proceed with the activity in question.

All of these new powers are potentially valuable, and when added to the existing enforcment powers to award compensation, seek injunctions, and investigate 'representative' or class complaints, Australia's Privacy Act now has one of the strongest 'regulatory toolkits' in the Asia-Pecific. But expanded powers are only valuable if they become credible through use, and credibility also requires transparency.

The transparency gaps

Unless all interested parties know the real tariff for breaching the Act (not just the formal possibilities), and that all of the enforcement toolkit is actually used, there are no effective feedback loops to discourage breaches, encourage complaints, and encourage compliance. Their use needs to be visible to individuals who want to use the Act to protect their rights, companies and agencies who must respond to complaints, and (most important) the lawyers and NGOs, advisers and intermediaries. If this is to be achieved after the 2014 empowerment, the Commissioner will have to improve the transparency of enforcement. This problem arises from five 'transparency gaps':[6]

---

[4] The only previous right of appeal was in relation to the quantum of awards of damages, and was only able to be used once.

[5] Australian Law Reform Commission *For Your Information* (ALRC 80, 2008), Recommendation 47-6. See Greenleaf and Waters, 2012.

[6] For more details see Graham Greenleaf 'Privacy law is toothless without greater transparency' *The Conversation* 12 March 2014 <http://theconversation.com/privacy-law-is-toothless-without-greater-transparency-22932>

(i) ***Silence from the courts*** After more than a quarter-century, Australia's federal *Privacy Act 1988* remains opaque, with only two slight cases illuminating its meaning. This odd situation stems from other gaps in the Act.

(ii) ***Determinations lacking*** Until now, the Commissioner's one significant power has been to make 'determinations' (formal decisions) under section 52, including compensation where appropriate, accompanied by a detailed explanation of the law, and naming the respondent. Although over 1500 complaints per year (2012/13 figures) are completed, only 2 in the last two years have resulted in formal decisions, and only eight since 2001, an average of less than one per year.

(iii) ***Dissatisfied complainants still have no right of appeal*** The new section 96(1)(c) right of appeal should allow AAT and court decisions to shine some light into corners of the Act. However, the track record of all Commissioners is that not even one person per year will get a decision to consider appealing against. Successive Commissioners have insisted that they will dismiss complaints if *they* think 'the respondent has dealt adequately with the complaint' (s41(2)(a)), even though the complainant disagrees. Dismissal blocks the right of appeal.

(iv) ***Lack of case summaries*** As a result, the Commissioner's published case notes on complaints mediated or discontinued have been the best information available. From 2001-2011 an average of 20 per year were published, but in January 2012 this also stopped, other than for a handful of reports of Commissioner-initiated investigations.

(v) ***Compensation payments remain unknown*** Compensation is the second most frequent remedy arising from mediated complaints, after apologies, amounting to an estimated $131,000 to 45 complainants in 2012/13, an average of $2,911. The fact that it is paid at all is largely unknown, and very difficult to accurately extract from the Commissioner's reports.

Perhaps the Privacy Commissioner will actively use his new powers, and in a transparent way, and will open the appellate door to privacy law. But the track record does not induce optimism.

The Commissioner's enforcement policy

The Office of the Australian Information Commissioner (OAIC) is developing a Privacy Regulatory Action Policy.[7] This otherwise valuable document does not yet cover some of the problems mentioned above, such as when complaints will be dismissed under section 41(2)(a) Despite an avowed Principle of 'transparency … about the regulatory outcomes it has achieved', it does not state an expected rate of case summaries, or improved communication of remedial outcomes. Transparency measures should be an essential component of an enforcement policy.

Mandatory breach reporting Bill returns

Mandatory data breach notification (MDBN) is still missing from the Privacy Act. The OAIC's *Data Breach Notification Guidelines* (2012) are voluntary. The Labor opposition has re-introduced into the Senate the *Privacy Amendment (Privacy Alerts) Bill 2014*. Debate on the Bill commenced on March 27, 2014.[8] A substantially identical Bill was originally introduced in 2013 by the then-Labor government, but lapsed in November 2013 at the end of the Parliamentary session prior to the change of government. The gist of the Bill is that all entities bound by the *Privacy Act 1988*, would be required to make various types of reports concerning a 'serious data breach.' Very complex provisions determine whether and when an organisation would need to make reports to the OAIC, to data subjects, on the organisation's website, in the press, or not at all. One of its strongest

[7] OAIC *Privacy Regulatory Action Policy* (draft, March 2014)

[8] See Parliament of Australia 'Privacy Amendment (Privacy Alerts) Bill 2014' <http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s958>

features is that any breaches of the reporting requirements would also constitute an 'interference with privacy', therefore bringing into play all of the enforcement provisions of the Privacy Act (including all those discussed above), and in effect constituting a right of data breach notification as a *de facto* 14th Australian Privacy Principle (APP).

Although the conservative parties supported the general principle of MDBN, they had reservations about the lack of definition of the terms 'serious breach' or 'serious harm' in the 2013 Bill. It now seems that, in government and in control of the House of Representatives, they will either oppose its passage or at least require further community consultation before it proceeds.[9] The future of the Bill is unclear.

Law reform enquiry into a statutory privacy action

The Australian Law Reform Commission (ALRC) was asked by the previous Labor government to report on 'the issue of prevention of and remedies for serious invasions of privacy in the digital era'. The Discussion Paper (DP 80)[10] containing its draft proposals was released in April 2014, and it is supposed to deliver its final report to the government by June 2014. Whether the current Liberal Attorney-General, well out on the right wing, will have any interest in privacy reforms seems unlikely. However, these reports often set the future agenda for reforms.

The key draft proposal is that a statutory cause of action for serious invasion of privacy (described as a tort) should be contained in a new federal Act, not in the existing Privacy Act. It would make actionable only invasions of privacy by: (a) intrusion upon the plaintiff's seclusion or private affairs (including by unlawful surveillance); or (b) misuse or disclosure of private information about the plaintiff (whether true or not). It would only extend to intentional or reckless invasions of privacy, and not to negligent actions. It would only be actionable where a person in the position of the plaintiff would have had a reasonable expectation of privacy, in all of the circumstances. The Act would include a long list of matters that the court could take into account. In determining whether the invasion of privacy was serious, a court could consider, among other things, whether the invasion of privacy was likely to be highly offensive, distressing or harmful to a person of ordinary sensibilities in the position of the plaintiff. The plaintiff would not be required to prove actual damage, the tort would be actionable per se if its elements were established.

Instead of separate public interest defence the court would have to be satisfied that the plaintiff's interest in privacy outweighs the defendant's interest in freedom of expression, and any broader public interest. The Act would also contain a non-exhaustive list of public interest matters which a court could consider. Various defences including absolute or qualified privilege, and exemptions for 'public documents' and fair report of proceedings of public concern, would significantly cut down the scope of the tort. A safe harbour scheme to protect internet intermediaries from liability for serious invasions of privacy committed by third party users of their services is proposed, with the conditions of its availability still unsettled. Factors would be listed that mitigate compensatory damages (encompassing emotional distress), including apologies, corrections, offers of amends, and reasonable attempts at settlement. Damages for non-economic loss would be capped as in defamation actions. All in all, this is a privacy tort restricted to the narrowest and most clearly justifiable circumstance, with the possibilities for abuse cut to the bone.

---

[9] Ashurst Australia 'Mandatory Data Breach Notification Bill re-introduced' (Ashurst, 25 March 2014)

[10] Australian Law Reform Commission *Serious Invasions of Privacy in the Digital Era* (DP 80, 31 March 2014) <http://www.alrc.gov.au/publications/serious-invasions-privacy-dp-80>.

Federal, state and territory courts would have jurisdiction in relation to the new tort. However, the Privacy Commissioner would not. Injunctions, correction orders, and accounts of profits would be among the remedies (other than compensation) that courts could order. The Australian Communications and Media Authority (ACMA) would also be given new powers, 'where there has been a privacy complaint under a broadcasting code of practice and where the ACMA determines that a broadcaster's act or conduct is a serious invasion of the complainant's privacy, to make a declaration that the complainant is entitled to a specified amount of compensation.' ACMA would be required to have regard to freedom of expression and the public interest. In addition, the Australian Information Commissioner (who formally exercises the Privacy Commissioner's roles) would be given the new function, in relation to court proceedings concerning interferences with privacy, of assisting the court as amicus curiae, or intervening in the proceedings, with the leave of the court.

The ALRC also hedges its bet, as its terms of reference allow it to do, by recommending that, if its preferred option of the statutory cause of action is not adopted, the following reforms should be made instead:

- Legislation should provide that an action for breach of confidence can be based on a serious invasion of privacy by the misuse, publication or disclosure of private information, and the court may award compensation for the claimant's emotional distress.
- Surveillance device laws and workplace surveillance laws should be made uniform throughout Australia, and should provide that a court may make orders to compensate or otherwise provide remedial relief to a victim of unlawful surveillance.
- There should be a new statutory tort of harassment.

Australia's federal structure raises complex questions of relationships between federal laws and stated and territory laws in the enactment of any of these laws, as they have to a large extent been state and territory laws in the past.

A not forgotten right

A new Australian Privacy Principle (APP), to be added to the Privacy Act, is also proposed by the ALRC. It would require those companies and agencies covered by the Act, to provide a simple mechanism for an individual to request destruction or de-identification of personal information that was provided to it by the individual, to give reasons if it refuses to do so, and to allow an appeal to a regulatory body (unspecified) to order an organisation to remove private information about an individual, whether provided by that individual or a third party, from a website or online service if the posting of the information constitutes a serious invasion of privacy. This 'right to be forgotten' would strengthen considerably the existing APPs.