The New Privacy Act: Six Months On

Nikki Macor Heath gives an update on the activities of the Office of the Australian Information Commissioner (OAIC) and Privacy Commissioner and enforcement of the Privacy Act since the commencement of the reformed legislation.

Just over six months ago, on 12 March 2014, substantial changes to the Privacy Act 1988 (Cth) came into effect. The changes included a new set of Australian Privacy Principles and a complete overhaul of the credit reporting regime. So what, if anything, has been the effect of these changes? Has the regulator capitalized on the significant promotion of privacy law that came along with the reform process? Or has the new regime, so far, proved an anti-climax?

There has as yet been no opportunity for the Privacy Commissioner to flex his new enforcement muscles, so it is fair to say the early impact of the reforms has fallen a bit flat. It is also likely that the restructuring and relocation resulting from the disbanding of the OAIC announced in the recent Federal budget will hamper the Commissioner's efforts in the coming months. However, it is clear that the changes have made an impact on at least some organisations, which have sought permission to do certain activities strictly in breach of the Privacy Act, or admitted to breaches from several years ago. There are also continuing efforts to explain and refine the operation of the new provisions through rules and guidance.

There has as yet been no opportunity for the Privacy Commissioner to flex his new enforcement muscles, so it is fair to say the early impact of the reforms has fallen a bit flat

Disbanding and relocating

In its 2014 budget, the Australian government announced its intention to disband the OAIC by 1 January 2015 in order to achieve savings of $10.2 million.[1]

The Privacy Commissioner, along with his support staff, will continue to regulate the Privacy Act from new premises, taking an independent statutory position within the Australian Human Rights Commission. This comes only four years after the OAIC was established and with the completion of the transition of the Privacy Commissioner's website from privacy.com.au to oaic.gov.au still very recent memory.

It is difficult to identify from the public budget papers what the specific funding impact on the Privacy Commissioner will be, as forward funding is only listed for the Australian Human Rights Commission as a whole. Given the general tone of cost cutting in the budget, it is likely that funding will take a hit. However, even assuming the Privacy Commissioner's resources remain unaffected, the administrative burden associated with the disbanding and relocation is likely to have an effect on substantive operations over the short to medium term.

Organisations seeking permission

Throughout the privacy reform process, the banking sector and in particular the Australia and New Zealand Banking Group Limited (ANZ), consistently expressed concerns regarding the reshaped cross-border disclosure principle and its potential impact on banks' international operations. Having seen the final form of APP 8, ANZ and, later, the Reserve Bank of Australia, applied to the Privacy Commissioner for public interest determinations to 'allow them and other authorized deposit taking institutions to disclose the personal information of a beneficiary of an international money transfer (IMT) to an overseas financial institution when processing an IMT without breaching' the APPs.[2] The concern was that, as a result of the complicated international transfer system and the practices of certain overseas financial institutions and regulatory bodies, personal information may need to be disclosed beyond what would be permissible under APP 8.

The Commissioner made two temporary public interest determinations, one specifically for ANZ, the other generalizing to the broader industry, in response to the ANZ's application. The Privacy (International Money Transfers) Temporary Public Interest Determination 2014 (No. 1) and Privacy (International Money Transfers) Generalising Determination 2014 (No. 1) commenced on 12 March 2014 and 'have the effect that ANZ and all other ADIs are taken not to breach APP 8.1 when disclosing personal information of the beneficiary of an IMT to an overseas financial institution for the purpose of remitting the relevant funds to the beneficiary's financial institution for payment'. The ADI will also not be held responsible for APP breaches (other than of APP 1) by an overseas financial institution in relation to that personal information. A consultation process regarding the issuing of permanent determinations closed for comment on 4 August 2014.

Organisations begging forgiveness

Shopping deals website Catch of the Day confessed in June 2014 to a data breach which occurred in 2011 and which had not previously been notified to the Privacy Commissioner.[3] With the Commissioner having asked for more information, it is unclear at this stage whether Catch of the Day has just discovered the breach, or has known about it for some time and was inspired by the publicity around privacy law or the new enforcement regime to proactively notify the Commissioner in an attempt to minimise the regulatory action it may face.

Organisations getting caught

No specific post-commencement breaches have yet been identified; however the Privacy Commissioner published several reports in relation to data breaches occurring prior to commencement of

1 Budget Paper No. 2: Budget Measures, http://www.budget.gov.au/2014-15/content/bp2/html/bp2_expense-05.htm.

2 'Consultation paper: International money transfers public interest determination applications', June 2014, http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/pdf/consultation-paper-international-money-transfers-pid-applications.pdf.

3 Catch of the Day data breach — statement, 21 July 2014, http://www.oaic.gov.au/news-and-events/statements/privacy-statements/catch-of-the-day-data-breach/catch-of-the-day-data-breach-statement.

the Privacy Act reforms, which remain subject to the National Privacy Principles (NPPs). These included own motion investigation reports into data breaches involving a hacking attack on online dating service provider Cupid Media Pty Ltd[4] and publication on search engines of records held by security authentication company Multicard Pty Ltd.[5] Both were found to have contravened NPP 4 requiring organisations to take reasonable steps to protect personal information. Cupid Media stored passwords in unencrypted plain text files, and Multicard had insufficient restrictions in place to prevent access to its files by automated search robots. Due to the cooperation and responsiveness of the company in each case, the Commissioner closed its investigation without taking further action.

The Privacy Commissioner also announced its cooperation with 27 other privacy regulators around the world to examine mobile applications to identify privacy issues, with a focus on 50 of Australia's most popular applications.[6] Results of the 'app sweep' will be published later in the year.

Tweaks to the credit reporting framework

As the focus of the most substantial and substantive changes as part of the privacy reforms, and a complex area to begin with, it is not surprising that the credit reporting framework has been the subject of some further refinement post-commencement. The Privacy (Credit Reporting) Code 2014 has been varied and the Privacy Commissioner made the Privacy (Credit Related Research) Rule 2014.

Even assuming the Privacy Commissioner's resources remain unaffected, the administrative burden associated with the disbanding and relocation is likely to have an effect on substantive operations over the short to medium term

Voluntary APP code

The Association of Market and Social Research Organisations (AMSRO) was first off the blocks releasing a voluntary privacy code for consultation. The draft Privacy (Market and Social Research) Code 2014 sets out how the APPs and Privacy Act are to be applied in the context of the use of personal information in social and market research by AMSRO members.[7]

New publications

The OAIC has been busy for some time publishing new guidance to assist organisations to adjust to the reformed privacy law. Since March, new publications have included a 'Guide to developing an APP privacy policy' and a 'Guide to undertaking privacy impact assessments'. A revised 'Guide to Information Security: 'Reasonable steps' to protect personal information' has been released for consultation.

The Heartbleed bug made headlines earlier this year, and the Privacy Commissioner took the opportunity to remind organisations of their obligations to take reasonable steps to protect personal information, including reviewing their IT security measures.[8] It is not clear whether any organisations are under investigation in connection with Heartbleed-related breaches, but the Commissioner encouraged affected organisations to assist users to change passwords after putting patches in place.

The Privacy Commissioner has also released a cautious comment on the government's data retention proposal (see 'Telecommunications Data Retention: A Step in the Right Direction?' in the March 2013 edition of the CAMLA Bulletin and recent media coverage) noting the risks of retaining a large amount of data and reiterating that organisations which are required to retain the data will be expected to comply with their APP and other Privacy Act obligations.[9]

Both were found to have contravened NPP 4 requiring organisations to take reasonable steps to protect personal information. Cupid Media stored passwords in unencrypted plain text files, and Multicard had insufficient restrictions in place to prevent access to its files by automated search robots

Nikki Macor Heath is a Corporate Lawyer at Adelaide Research and Innovation Pty Ltd. The views expressed in this article are the views of the author only and do not represent the views of any organisation.

---

4 'Cupid Media Pty Ltd: Own motion investigation report', June 2014, http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/cupid-omi.

5 Multicard Pty Ltd: Own motion investigation report, May 2014, http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/multicard-omi.

6 'Privacy Awareness Week ends, global sweep of apps begins!', 9 May 2014, http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-awareness-week-ends-global-sweep-of-apps-begins.

7 'Privacy – Market and Social Research – Code 2014', http://www.amsro.com.au/member-services/privacy/privacy-market-and-social-research-code-2014.

8 'Heartbleed bug', 11 April 2014, http://www.oaic.gov.au/news-and-events/statements/privacy-statements/heartbleed-bug/heartbleed-bug.

9 'Australian Government's data retention proposal — statement', 8 August 2014, http://www.oaic.gov.au/news-and-events/statements/privacy-statements/australian-governments-data-retention-proposal/australian-government-s-data-retention-proposal.