Chapter Six

Privacy policy and law reform

Chapter Six
Privacy policy and law reform

Overview

The Office of the Australian Information Commissioner (OAIC) provides strategic policy advice on the application of the *Privacy Act 1988* (Privacy Act) to Australian and ACT Government agencies, the Norfolk Island Administration and private sector organisations.

In 2013–14, a key focus for the OAIC was to provide advice that enabled agencies and organisations to understand their obligations following the commencement of the privacy law reforms made by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Privacy Amendment Act) on 12 March 2014.

The OAIC also continued its work in the eHealth area as the independent regulator of the privacy aspects of the Personally Controlled Electronic Health Records (PCEHR) system and the Health Identifiers (HI) service.

The OAIC provided advice to Commonwealth and state and territory governments, international privacy regulators, privacy advocates, private sector organisations, peak industry bodies, and members of the public. This advice covered a wide range of privacy related matters, and involved responding to specific requests for advice, legislative proposals and reviews, and significant new Government policies and projects.

Privacy law reform

On 12 March 2014, amendments to the Privacy Act made by the Privacy Amendment Act came into force. These amendments included the replacement of the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) with the Australian Privacy Principles (APPs), the amendment of the Part IIIA credit reporting provisions and new regulatory powers for the OAIC.

The OAIC produced an extensive range of guidelines and legislative instruments to assist agencies, organisations and the public to understand their privacy obligations and rights. Additionally, the OAIC responded to specific privacy enquiries from Australian Government agencies, private sector bodies and individuals.

Further information about the privacy law reform changes and materials that the OAIC produced are detailed below.

Australian Privacy Principles

The APPs are legally binding principles which form the cornerstone of the privacy protection framework in the Privacy Act. The APPs regulate the handling of personal information by both Australian Government agencies and private sector organisations (collectively known as 'APP entities').

Australian Privacy Principles guidelines

The OAIC released a final version of its *Australian Privacy Principles guidelines* (APP guidelines) in February 2014. The APP guidelines are an essential and comprehensive reference document to assist agencies, organisations and the public in understanding the APPs.

The APP guidelines outline the mandatory requirements in the APPs and the OAIC's interpretation of the APPs (including the matters the OAIC may take into account when exercising functions and powers relating to the APPs). Additionally, the APP guidelines include examples that explain how the APPs may apply to particular circumstances to assist compliance with the mandatory requirements as well as good privacy practice suggestions.

The APP guidelines represent the completion of a significant amount of collaborative work both internally and with external stakeholders. The OAIC conducted a period of targeted consultation, before consulting publicly on the guidance. Public consultation took place in three stages over a four month period. In total, the OAIC received 96 submissions to its public consultation from a range of contributors, including from individuals as well as APP entities and peak bodies across different sectors.

Guidance about APP privacy policies

Every entity that is bound by the Privacy Act is required to have a clearly expressed and up-to-date APP privacy policy describing how it manages personal information.

The OAIC produced the *Guide to developing an APP privacy policy* to assist APP entities to comply with APP 1, and to inform individuals about what they should be looking for in a privacy policy. The guide provides some tips, a checklist of important considerations, and a process for developing an APP privacy policy. The OAIC also developed a 'What to look for in a privacy policy' poster for individuals.

Enhanced powers

The privacy reforms gave the Commissioners access to new enforcement powers. The Information and Privacy Commissioners issued a joint regulatory statement in late February 2014 explaining the OAIC's enforcement approach.

The OAIC also began developing a regulatory action policy that explains the OAIC's range of powers and its approach to using its privacy regulatory powers.

Regulatory action policy

The OAIC's *Privacy regulatory action policy* sets out information including:

- the OAIC's goal of, and guiding principles for, taking privacy regulatory action

- the OAIC's approach to regulatory action
- how the OAIC decides whether to take regulatory action in a particular situation
- when privacy regulatory actions may be publicly communicated.

The draft policy was released for a public exposure period in March 2014 and the OAIC received comments from various stakeholders including peak industry bodies. The OAIC expects the finalised policy to be published in the second half of 2014.

Credit reporting laws

The purpose of the consumer credit reporting system is to balance protecting an individual's personal information with the need for credit providers to have enough information to help them decide whether or not to give credit to an individual.

The new credit reporting provisions in Part IIIA of the Privacy Act govern the use of credit information relating to notifications, data quality, access and correction and complaints. The revised system also covers the collection of repayment history information, a simplified and enhanced correction and complaints process, and civil penalties for breaches of certain credit reporting provisions.

The credit reporting reforms were supplemented by an industry developed code of practice, known as the *Privacy (Credit Reporting) Code 294* (CR code), which was registered by the OAIC within the reporting period. The CR code requires all credit reporting bodies to publish statistical and other information about credit reporting activity on their websites by 31 August each year.

Credit reporting 'know your rights' fact sheet series

In May 2014, the OAIC released a comprehensive series of 15 fact sheets about credit reporting, called *Credit reporting: Know your rights*. The fact sheets outline what individuals need to know about how their personal information can be handled in the Australian credit reporting system. This is the first comprehensive set of educative resources on credit reporting produced by the OAIC, and is complemented by a list of frequently asked questions.

External dispute resolution

External dispute resolution (EDR) schemes assist individuals by receiving complaints about the EDR member organisations, and providing independent dispute resolution services to resolve those complaints. The Privacy Act recognises the benefit of individuals bringing their complaints to an EDR scheme that has extensive experience in a particular industry, before it is brought to the OAIC, if necessary.

The Information Commissioner can recognise EDR schemes to handle particular privacy-related complaints under the Privacy Act. In order to be recognised, EDR schemes must demonstrate their accessibility, independence, fairness, accountability, efficiency and effectiveness.

Guidelines for recognising EDR schemes

During the reporting period the Commissioner developed *Guidelines for recognising EDR schemes* (EDR Guidelines). These Guidelines outline the matters that the Commissioner must take into account in considering whether to recognise an EDR scheme, the steps an EDR scheme should take to apply for recognition, and the general conditions for ongoing EDR recognition. The Commissioner consulted with EDR schemes in developing the EDR Guidelines.

As at 30 June 2014 the Privacy Commissioner had recognised seven EDR schemes. The EDR Guidelines require recognised EDR schemes to provide information about privacy related complaints to the Commissioner by 31 July each year for inclusion in this annual report, however due to the short time since the privacy reforms commenced the OAIC has waived the requirement for this financial year.

Codes

APP codes

The Privacy Act allows the OAIC to register binding APP codes that are in the public interest. APP codes do not replace the relevant provisions of the Privacy Act, but operate in addition to the requirements of the APPs.

APP codes can be developed by entities on their own initiative, on request from the OAIC, or developed by the OAIC directly. An APP code can provide greater clarity on how the APPs apply in a particular industry, or be used to incorporate higher standards for privacy protection than the Privacy Act requires.

As at 30 June 2014 no APP codes had been registered. However, the OAIC had consulted with the Association of Market and Social Research Organisation (AMSRO) about the development of a new APP code. Further information regarding AMSRO's code can be found under 'Advice to the private sector'.

Guidelines for developing codes

In September 2013, the OAIC released the *Guidelines for developing codes — issued under Part IIIB of the Privacy Act 1988* to assist entities to decide whether it is appropriate for them to develop an APP code, and to outline matters that need to be addressed in the development and registration of an APP code.

CR code

The Privacy Act also requires the development of a code of practice about credit reporting, called the CR code. The CR code sets out how the Privacy Act's credit reporting provisions are to be applied or complied with by credit reporting bodies (CRBs), credit providers and other entities bound by Part IIIA. Importantly, there must always be a registered CR code.

In December 2012 the Australian Privacy Commissioner requested the Australian Retail Credit Association (ARCA) develop a new credit reporting privacy code. Following extensive consultation with industry representatives, consumer advocates and the OAIC, the *Privacy (Credit Reporting) Code 2014* was registered on the OAIC's Codes Register on 22 January 2014.

Additional Privacy Law Resources

Following the privacy law reforms, the OAIC updated a number of resources including the *Guide to undertaking privacy impact assessments* and the *Privacy public interest determination guide*.

Guide to undertaking privacy impact assessments

In May 2014, the OAIC released a revised *Guide to undertaking privacy impact assessments* (PIA guide). A privacy impact assessment (PIA) is a way entities can assess a project to understand the impacts that the project might have on the privacy of individuals. Undertaking a PIA assists entities to manage, minimise or eliminate those impacts.

The PIA guide was revised to reflect the introduction of the APPs and the introduction of a new power for the OAIC to direct Australian Government agencies to undertake a PIA. The OAIC also considered research on best practice in undertaking PIAs and incorporated elements from PIA guides from other jurisdictions.

Privacy public interest determination guide

The OAIC has the power to make a determination that an act or practice of an agency or a private sector organisation, which would generally be a breach of an APP or a registered APP code, will instead not be regarded as a breach. This is known as a privacy public interest determination (PID).

In June 2014, the OAIC released an updated *Privacy public interest determination guide* to reflect the new law, including the OAIC's powers in relation to PIDs and the APPs. The guide emphasises the importance of an APP entity consulting with the OAIC before applying for a PID.

Privacy (Credit Related Research) Rule 2014

The Privacy Act allows the Commissioner to make rules which allow credit reporting bodies to use or disclose de-identified information for the purposes of conducting research in relation to credit. In accordance with s 20M(3) of the Privacy Act, the Commissioner developed the *Privacy (Credit Related Research) Rule 2014* to this effect.

Further information regarding the *Privacy (Credit Related Research) Rule 2014* can be found under 'New legislative instruments' below.

Privacy (Persons Reported as Missing) Rule 2014

The reforms to the Privacy Act introduced a range of exceptions to the APPs, known as permitted general situations. One particular permitted general situation allows an APP entity to collect, use or disclose personal information to assist in locating a person who has been reported as missing, provided the entity acts in accordance with rules made under s 16A(2).

The OAIC developed the *Privacy (Persons Reported as Missing) Rule 2014*, which outlines the circumstances in which APP entities are permitted to collect sensitive information and use or disclose personal information to locate a person reported as missing. Further information regarding the *Privacy (Persons Reported as Missing) Rule 2014* can be found under 'New legislative instruments'.

eHealth

The 2013–14 financial year was the second year of operation of the Personally Controlled Electronic Health Record (PCEHR) system, established under the *Personally Controlled Electronic Health Records Act 2012* (PCEHR Act). This year was also the fourth year of the Healthcare Identifiers (HI) service, an important foundation for the PCEHR system and eHealth generally. The HI service is established under the *Healthcare Identifiers Act 2010* (HI Act).

The handling of individuals' personal information is at the core of both the PCEHR system and the HI service (collectively referred to as eHealth in this report). In recognition of the special sensitivity of health information, both the PCEHR and HI Acts contain provisions protecting and restricting the collection, use and disclosure of personal information. The OAIC administers those provisions as the independent regulator of the privacy aspects of the PCEHR system and HI service.

The OAIC's eHealth activities were carried out under a Memorandum of Understanding (MOU) with the Department of Health (Health). In accordance with the MOU, the OAIC carried out a full program of eHealth related work, including:

- commencement of five audits relating to the PCEHR system and HI service, and completion of three audits/assessments
- establishment of the *Agreement for information sharing and complaint referral relating to the personally controlled electronic (eHealth) record system between the OAIC and the System Operator*, in consultation with Health
- providing input to the independent review of the PCEHR system
- responding to two mandatory data breach notifications from the PCEHR System Operator
- reviewing and developing guidance materials for a range of audiences
- training and developing OAIC staff in the eHealth privacy regulatory framework.

More information on this MOU can be found in Appendix Five.

Advice to Australian Government agencies

The OAIC provided policy advice to Australian Government agencies, including advice on the management of personal information through legislation and on specific policy proposals. A selection of the policy advices provided in 2013–14 appears below.

Serious invasions of privacy in the digital era

The Privacy Commissioner was a member of the Advisory Committee for the Australian Law Reform Commission (ALRC) inquiry into serious invasions of privacy in the digital era.

In addition, the OAIC provided comments to the inquiry in response to the ALRC's issues paper and discussion paper. The OAIC took the view that the most effective way to address serious invasions of privacy (beyond those presently covered by the Privacy Act) would be a complaints model. Under this approach, a person whose privacy has been invaded would initially lodge a complaint with the OAIC rather than starting court proceedings. This approach would be more accessible to individuals and would encourage informal and low-cost resolution of disputes through conciliation. It would also use the OAIC's existing expertise in privacy issues and in conciliating complaints. A court proceeding may be an option at a later stage in resolving a grievance.

Customer due diligence provisions of the Anti-Money Laundering/ Counter-Terrorism Financing Rules

The Australian Transactions Reports and Analysis Centre (AUSTRAC) conducted a consultation on proposed changes to the customer due diligence (CDD) provisions of the *Anti-Money Laundering/Counter-Terrorism Financing Rules 2006* (AML/CTF Rules).

The OAIC reviewed the proposals to allow reporting entities to collect personal information from identified beneficial owners, and to rely on third parties to collect CDD information. The OAIC advised AUSTRAC on its interpretation of the relationship between the APPs and the proposals, which raised privacy issues about the collection and sharing of personal information. The OAIC remained involved in the consultation process, in particular by providing comment on AUSTRAC's response to a PIA on the proposed changes to the CDD provisions, until the new CDD provisions took effect on 1 June 2014.

Big Data

The OAIC participated in the inter-agency Big Data Strategy Working Group, led by the Australian Government Information Management Office. The Big Data Strategy intends to guide the use of 'Big Data' — high volume data-driven analytical tools — to assist and improve Australian Government agencies' operations. The OAIC participated in the development of the whole-of-government Big Data Strategy to help ensure that it incorporated the obligations of Australian Government agencies under the Privacy Act, and reflected best privacy and information management practice.

Interaction between the new credit reporting laws and financial hardship laws

The OAIC participated in a multi-agency roundtable on 'for-profit' financial difficulty businesses, with a key focus on 'credit repair' organisations. Following this roundtable the Australian Securities and Investments Commission (ASIC) sought feedback from the OAIC on a possible definition of 'credit repair' services, given the possible overlap with terms defined in the Privacy Act. In response, the OAIC provided advice on the language proposed by ASIC, and also whether the proposed definition would be likely to capture the full range of activities undertaken by 'credit repair' organisations.

Health and medical research guidelines

Under the Privacy Act, the National Health and Medical Research Council (NHMRC) may issue guidelines that relate to the protection of privacy by agencies in the conduct of medical research (s 95), the handling of health information for the purposes of research, the compilation or analysis of statistics, or health service management (s 95A), and the use and disclosure of genetic information by health practitioners (s 95AA).

The Privacy Act reforms that commenced on 12 March 2014 meant that updates to these guidelines were required to ensure that they reflected the amended Privacy Act and would be current and operational. The OAIC worked with the NHMRC to identify the updates required to the three guidelines prior to the commencement of the reforms. The guidelines were registered on the Federal Register of Legislative Instruments on 11 March 2014.

Membership of EDR schemes

As a result of amendments to the Privacy Act, certain organisations known as credit providers are now required to become a member of an EDR scheme that has been recognised by the OAIC. Membership to an EDR scheme will allow a credit provider to engage with the credit reporting system. This requirement became problematic for certain energy and water service providers whose current EDR schemes are unable to seek recognition as a result of statutory restrictions.

Following the OAIC's release of guidelines relating to the recognition of EDR schemes, the OAIC liaised with EDR schemes that were unable to seek recognition under the Privacy Act. The OAIC then provided advice to the Attorney-General's Department about the barriers preventing EDR schemes from seeking recognition, and the implications these barriers would have on individuals, energy and water providers, and the credit reporting system generally. The OAIC also provided advice on possible resolutions and transitional arrangements to allow these credit providers to continue accessing the credit reporting system.

Part 13 of the Telecommunications Act

The OAIC provided advice to the Department of Communications on proposed reforms to Part 13 of the *Telecommunications Act 1997*, as part of the Australian Government's deregulation agenda. The OAIC also participated in stakeholder forums run by the Department of Communications. This work will continue in 2014–15.

Department of Human Services MOU

The OAIC and the Department of Human Services (DHS) entered into an MOU to cover the 2013–14 financial year. Under the MOU, the OAIC provided dedicated policy advice and assistance to DHS in relation to the interpretation and management of personal information privacy obligations by DHS in connection with the administration and delivery of its payments and services. This included providing advice on DHS's myGov client access portal.

More information about the MOU can be found at Appendix Five.

Advice to Australian Capital Territory agencies

The OAIC provides advice to Australian Capital Territory (ACT) Government agencies on privacy issues under an MOU. More information about the MOU can be found at Appendix Five.

Territory Privacy Principles

The OAIC undertook to compare the Territory Privacy Principles (TPPs) contained in schedule 1 to the Information Privacy Bill 2014 (ACT) with the APPs contained in schedule 1 of the Privacy Act, following a meeting with the ACT Government's Justice and Community Safety Directorate (JACS).

The OAIC conducted the analysis comparing the TPPs with the APPs for any material difference. The OAIC found some differences between the TPPs and APPs. The OAIC advised JACS of these differences.

The *Information Privacy Act 2014* (ACT), including the Territory Privacy Principles, will commence on 1 September 2014.

Advice to the private sector

The OAIC worked collaboratively with business and not-for-profits to promote an understanding and acceptance of the new privacy laws and APPs. During 2013–14, the OAIC provided advice to private sector entities on a variety of matters.

APP 7 and communications between general practitioners and patients

APP 7 introduced new obligations for organisations, including healthcare providers, around direct marketing. Advice from the OAIC was sought on the application of APP 7 to communications between health practitioners and their patients.

The OAIC advised that some health practitioner communication activities may meet the definition of direct marketing (the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services).

Public reporting of payments to healthcare providers

Medicines Australia sought advice from the OAIC about the privacy implications of a proposed transparency measure that would involve public reporting about pharmaceutical companies' payments and other transfers of value to individual healthcare professionals. The OAIC advised on a number of aspects of the proposal, including the distinction between primary and secondary purposes of collection, exceptions permitting the use and disclosure of personal information for a secondary purpose, consent issues, and adoption, use and disclosure of government related identifiers. The OAIC also provided advice to the Australian Medical Association about the proposal.

Google

During the course of 2013–14, the OAIC continued its engagement with Google on the development of the Google Glass wearable computing device. Previously the OAIC, in conjunction with other national privacy regulators, wrote to Google to raise privacy issues about the development of Google Glass. Specifically, the signatories asked Google to address concerns about what information Google collects through Google Glass, what information it shares with third parties and what privacy safeguards Google and application developers are putting in place.

In 2013–14, the OAIC's interaction with Google included an opportunity for the Privacy Commissioner to participate in a demonstration of Google Glass. The OAIC also received briefings from Google regarding products in development and new products during the course of 2013–14. In the course of these briefings, the OAIC provided verbal comments to help Google achieve better privacy practice.

Facebook

The OAIC received regular briefings from Facebook in 2013–14 regarding new products and products in development. In the course of these briefings, the OAIC provided verbal comments to help Facebook achieve better privacy practice.

Advice to small business on credit reporting laws

Following recent changes to Australia's credit reporting laws, the OAIC received a number of enquiries about the definition and obligations of a 'credit provider' in the Privacy Act.

In response, the OAIC provided advice that a small business (or small business operator) that falls within the definition of a credit provider must have a credit reporting policy outlining how it manages credit information. However, small businesses that are credit providers and do not engage with the credit reporting system may be able to comply with these obligations by publishing a short statement that states the business handles credit information in certain circumstances, but does not disclose this information to credit reporting bodies. The OAIC further advised that a credit provider that wishes to engage in the credit reporting system must be a member of a recognised EDR scheme, unless an exemption to that obligation exists in the privacy regulations.

Market and Social Research Privacy Code

The Market and Social Research Privacy Code, previously registered under Part IIIAA of the Privacy Act, was no longer a registered code under the Privacy Act after 12 March 2014.

The Association of Market and Social Research Organisations (AMSRO) advised the OAIC that they intended to register a new APP code in accordance with the Privacy Amendment Act. The OAIC advised AMSRO on the process for developing and registering a code under the revised Privacy Act. At the end of the reporting period, AMSRO had publicly consulted on the proposed APP code.

Involvement in cross-government forums

The OAIC is a member of several cross-government committees and forums. The OAIC engages with other members and state and territory government agencies to provide advice on the privacy obligations relevant to that committee or forum.

The National Identity Security Coordination Group

The OAIC is a member of the National Identity Security Coordination Group (NISCG), coordinated by the Attorney-General's Department (AGD). The NISCG consists of representatives from the Australian and state and territory government agencies with key roles in identity management. The NISCG was established to coordinate and implement the National Identity Security Strategy.

The OAIC is also a member of the Commonwealth Reference Group on Identity Security (CRG), which was established to facilitate a whole-of-Government contribution to the National Identity Security Strategy. The OAIC provides privacy policy advice to these groups.

National Biometrics Interoperability Framework Steering Committee

The OAIC continued to participate in the National Biometrics Interoperability Framework Steering Committee. The purpose of the Committee is to guide the biometric centres of expertise managing and overseeing the National Biometric Interoperability Framework (NBIF), and to promote biometric interoperability across the Australia Government. The OAIC provides policy advice on the privacy considerations to be taken into account in the development of the NBIF, and other biometrics projects.

AUSTRAC Privacy Consultative Committee

The OAIC is a member of the AUSTRAC Privacy Consultative Committee, an advisory committee to the AUSTRAC Chief Executive Officer (CEO). The Privacy Consultative Committee comprises revenue, law enforcement, privacy and civil liberties representatives to promote understanding of issues and develop positions concerning privacy, civil liberties and related matters. The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) requires the AUSTRAC CEO to have regard to privacy, and consult with the OAIC in performing functions under the AML/CTF Act. The Privacy Consultative Committee is one of the means by which the AUSTRAC CEO fulfils these obligations.

Arrangement with state and territory health and privacy regulators

In 2012–13, the OAIC developed an information sharing and complaints referral arrangement between the OAIC and state and territory health and privacy regulators (the Arrangement), following extensive consultation with other regulators. The Arrangement establishes a protocol for referring and handling eHealth complaints where there is overlapping or concurrent jurisdiction, or where a complaint is made to the wrong regulator.

In April 2014, the Information and Privacy Commissioner New South Wales agreed to become a party to the Arrangement, joining the other parties:

- OAIC
- Office of the Information Commissioner, Queensland
- Health Services Commissioner, ACT Human Rights Commission
- Office of the Health Services Commissioner, Victoria
- South Australian Health and Community Services Complaints Commissioner.

In May 2014, the OAIC wrote to all parties to the Arrangement seeking comment on the Arrangement. The terms of the Arrangement include a review of the Arrangement by 30 June 2014 (and every two years subsequently). None of the parties indicated that any changes were required, and the OAIC wrote to all parties in June 2014 confirming that the Arrangement would continue in its current form.

Advice to other jurisdictions

The OAIC provides advice to other jurisdictions as part of its activities, both internationally and domestically.

During 2013–14, the OAIC continued to participate actively in a number of international privacy and data protection forums. Participation in these forums enables the OAIC to build collaborative relationships and remain aware of emerging international privacy protection issues. Below are some of the specific interactions the OAIC had with these forums during 2013–14.

During 2013–14, under the Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement the OAIC worked with regulators including the Data Protection Commissioner of Ireland and the Office of the Privacy Commissioner of Canada on data breach matters that had international ramifications.

The OAIC actively participated in discussions with the Asia Pacific Privacy Authorities (APPA) Forum on emerging privacy technology, including through APPA's Technology Working Group. The OAIC also participated in regular meetings of the Organisation for Economic Cooperation and Development's Global Privacy Enforcement Network Asia-Pacific subgroup, in which privacy regulators discuss their experiences and emerging trends, and share expertise.

Domestically, the OAIC provided policy advice to state and territory governments in relation to the sharing and handling of personal information.

More detailed information about these forums can be found in Chapter 4.

Advice to the Ombudsman South Australia on Information Sharing Guidelines

The OAIC provided advice to the Ombudsman SA on the compatibility of the *Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children, Young People and their Families* and the APPs. The OAIC advised the Ombudsman SA on its interpretation of when a disclosure of an individual's personal information can occur without the consent of that individual, and the consistency of the interpretation contained within the Information Sharing Guidelines against the APP 6 guideline developed by the OAIC.

Advice to Queensland Government privacy review

The OAIC provided a submission to the Queensland Government's review of the *Information Privacy Act 2009* (Qld) and the *Right to Information Act 2009* (Qld). The OAIC's submission emphasised the value of national consistency in privacy regulation across Australian jurisdictions, and outlined the upcoming reforms to the Privacy Act. It also provided information on the recent review of the Commonwealth freedom of information regime (the Hawke review), and noted key elements of the OAIC's submission to that review.

Advice to Northern Territory Department of Health My eHealth Record database

The Northern Territory Department of Health (NT Health) requested advice from the OAIC about private healthcare providers' obligations under APP 9 when collecting, using and disclosing Medicare numbers through the NT *My eHealth* Record database. This was intended to assist in identifying duplicate records and enable searches for Individual Healthcare Identifiers.

Trans-Pacific Partnership Free Trade Agreement

The Trans-Pacific Partnership, also known as the Trans-Pacific Strategic Economic Partnership Agreement, is a multilateral free trade agreement that aims to integrate the economies of the Asia Pacific region. Membership includes Brunei, Chile, New Zealand, Singapore, Vietnam, Malaysia, Peru, United States, and Australia.

The OAIC provided advice to the Australian Government representatives on the privacy considerations of the e-commerce chapter of the Trans-Pacific Partnership. Most recently, the OAIC provided advice on the Trans-Pacific Partnership's interaction with APP 8 — Cross-border disclosure of information.

New legislative instruments

Under the Privacy Act, the Information Commissioner has power to make certain legislative instruments. When making those legislative instruments, the Commissioner is required to comply with the requirements of the *Legislative Instruments Act 2003*. All legislative instruments finalised during 2013–14 were registered on the Federal Register of Legislative Instruments (FRLI).

Privacy (Credit Reporting) Code 2014

The *Privacy (Credit Reporting) Code 2014* (CR code) was registered on OAIC's Codes Register on 22 January 2014. The CR code is a written code of practice about credit reporting that supplements the credit reporting provisions in the Privacy Act. As part of the reforms to the Privacy Act, the OAIC is required to ensure that there is a registered CR code at all times after 12 March 2014.

On 3 April and 24 April 2014, the OAIC registered variations of the CR code on the OAIC's Codes Register. The first variation was requested by the code developer, ARCA, and extended the period of time before an overdue payment can be listed as repayment history information on an individual's credit report. The second variation was made on the OAIC's own initiative and made some minor technical variations, including the insertion of a repeal provision. The CR code and its variations have also been registered on FRLI.

Privacy (Persons Reported as Missing) Rule 2014

The OAIC registered the *Privacy (Persons Reported as Missing) Rule 2014* (the Rule) on FRLI on 3 March 2014. The Rule sets out when, under permitted circumstances, an APP entity may collect sensitive information about a person reported as missing and an APP entity may use or disclose personal information about a person reported as missing.

The OAIC published a *Guide to the Privacy (Persons reported as Missing) Rule 2014* (the Guide), to assist APP entities and others to understand and use the Rule. The Guide outlines the mandatory requirements of the Privacy Act and the Rule, examples that explain how these may apply, as well as good privacy practice.

Privacy (Credit Related Research) Rule 2014

The *Privacy (Credit Related Research) Rule 2014* (the Rule) was registered on FRLI on 7 May 2014. The purpose of the Rule is to permit the use or disclosure of de-identified information in credit related research, where it is in the public interest. The use or disclosure of de-identified information by credit reporting bodies, when conducting credit related research, is permitted when that research complies with the Rule and s 20M of the Privacy Act.

The OAIC consulted with industry and other government agencies to develop the Rule. The Rule sets out the permitted purposes for conducting credit related research, reasonable steps to take to de-identify credit reporting information and the restrictions on disclosing de-identified credit reporting information. Most importantly,

the re-identification of de-identified credit reporting information is prohibited. A credit reporting body must also include a statement in its privacy policy on the management of de-identified information.

Public interest determinations

Part VI of the Privacy Act gives the Information Commissioner the power to make a determination that an act or practice of an Australian or ACT Government agency, or a private sector organisation, which may constitute a breach of an APP or an approved APP code, shall be regarded as not breaching that principle or approved code for the purposes of the Privacy Act. This is known as a public interest determination (PID).

Review of existing PIDs for privacy reforms

Before the commencement of the Privacy Act reforms, the OAIC made the *Privacy Public Interest (Enhancing Privacy Protection) Amendment and Repeal Determination 2014*. This determination amended and repealed 11 PIDs that were in force immediately prior to commencement of the Privacy Amendment Act. In particular, the determination:

- made minor amendments to PIDs 3A, 5, 12 and 12A to ensure that, on commencement of the Privacy Amendment Act, each determination would operate in an identical fashion to the way it operated immediately before commencement
- repealed PIDs 4, 7, 11, 11A, 13 and 13A as the acts and practices covered by these determinations would not breach the Australian Privacy Principles in the amended Privacy Act
- repealed PID 8 as the act or practice covered by the determination was complete and the determination was no longer required.

Before making these determinations, the OAIC gave notice to each original applicant of the proposed amendment or repeal of their PID. As the effects of the determination were of a minor nature and did not substantially alter existing arrangements, the OAIC was satisfied that further consultation was unnecessary.

International Money Transfers

On 12 March and 16 May 2014, the OAIC made three temporary PIDs in response to applications by the Australia and New Zealand Banking Group Limited and the Reserve Bank of Australia. The PIDs allow the current well-established international money transfer (IMT) process to continue by permitting the disclosure of the personal information of a beneficiary of an IMT to an overseas financial institution when processing an IMT, without breaching the APPs. The temporary PIDs will apply for a period of up to 12 months, while the OAIC considers whether longer-term PIDs should be made.

Submission list

In 2013–14, the OAIC made several privacy submissions to inquiries being undertaken by parliamentary committees and government agencies. The published submissions made by the OAIC during 2013–14 are listed below.

Privacy law reform

- *Discussion Paper 80: Serious invasions of privacy in the digital era* — submission to the Australian Law Reform Commission (from May 2014)
- *Issues Paper 43: Serious invasions of privacy in the digital era* — submission to the Australian Law Reform Commission (December 2013)
- *Review of the Information Privacy Act 2009 (Qld) and Right to Information Act 2009 (Qld)* — submission to Queensland Department of Justice and Attorney-General.

Employment

- *Review of Subdivision A of Division 6 of Part VIIC of the Crimes Act 1914 — the working with children exclusion* — submission to the Attorney-General's Department
- *Notification of employment decisions in the Gazette — a discussion paper* — submission to the Australian Public Service Commission.

Finance

- Statutory review of the *Personal Property Securities Act 2009* — submission to Ashurst.

Health

- *Revision of Chapter 2.3 of National Statement on Ethical Conduct in Human Research* — submission to the National Health and Medical Research Council.

National security

- Proposed amendment to the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1)*: Customer Due Diligence provisions — submission to AUSTRAC
- Review of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* — submission to AUSTRAC.

Transport

- *Proposed Compliance Framework for Heavy Vehicle Telematics* — submission to the National Transport Commission.

Telecommunications

- Inquiry into comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* — submission to the Senate Legal and Constitutional Affairs Committee.

Online Services

- Review of Whois policy for .au domain names – submission to .au Domain Administration Ltd
- Study of Whois Privacy and Proxy Service Abuse – submission to the Internet Corporation for Assigned Names and Numbers.