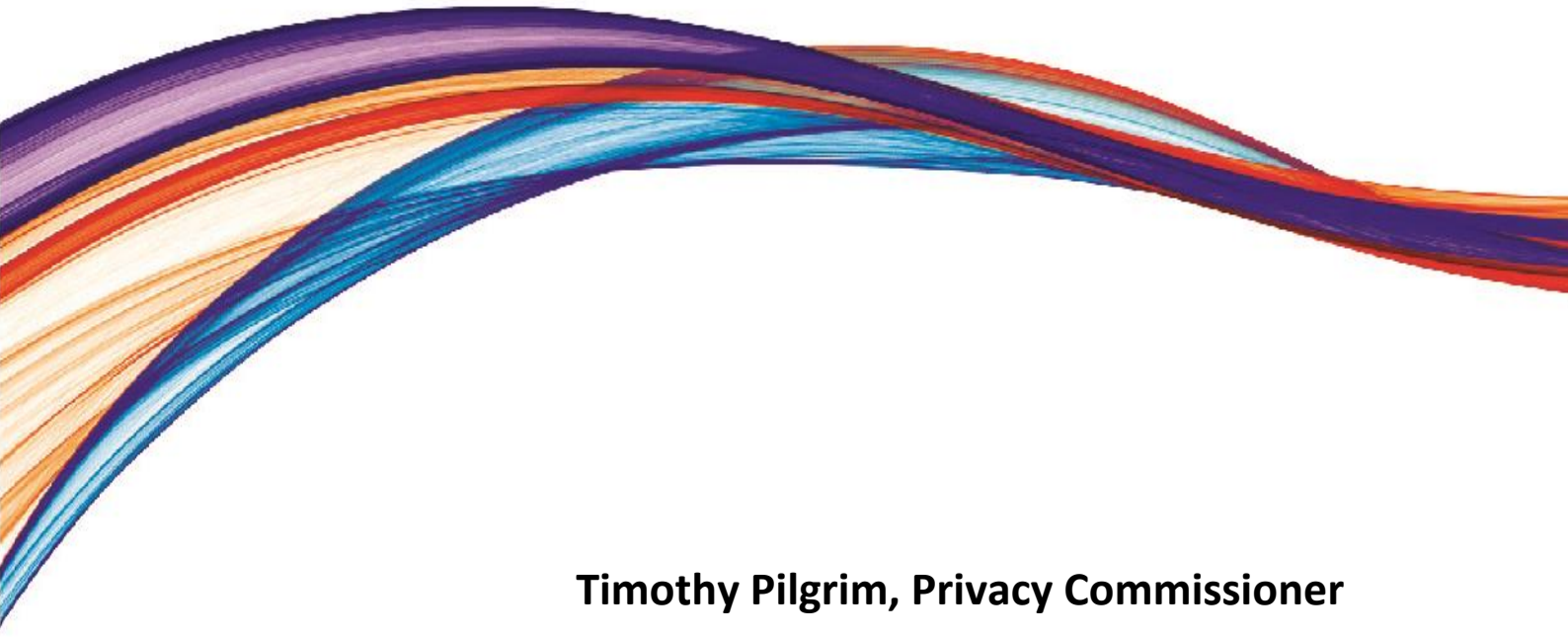
Australian Government

Office of the Australian Information Commissioner

Financial System Inquiry

Submission responding to the Inquiry's interim report

August 2014



Timothy Pilgrim, Privacy Commissioner

Contents

Key messages

Privacy regulation and the financial system

Consumer confidence, to a large degree, rests on responsible privacy practice in the financial sector. This is even more so in an age of online banking and digital services.

The Office of the Australian Information Commissioner (OAIC) plays a pivotal role in assuring consumers that privacy protections will be enforced, and alleged misuse of personal information will be investigated. In addition, the OAIC engages with regulated entities to provide guidance, promote best practice compliance and identify and seek to address privacy concerns as they arise.

The OAIC is the primary regulator for personal information handling across all large private sector and not-for-profit organisations, some smaller organisations and most Australian Government agencies. [1] This provides a strong framework for consistent privacy regulation and enforcement across all sectors in Australia.

A strong privacy regulatory framework will encourage strong consumer confidence. For that reason:

- the Australian Privacy Principles (APPs) and credit reporting provisions in the Privacy Act 1988 should continue to be the central regulatory framework for personal information handling in Australia across all sectors including the financial sector
- privacy issues arising in relation to a particular sector or technology can be dealt with by the registration of a binding APP code, if appropriate; an APP code would build on the APPs and avoid fragmentation
- the OAIC should continue to be the primary privacy regulator for the financial sector and should be consulted on significant changes to, or the introduction of, regulation or policies affecting the handling of personal information.

New information handling initiatives in the financial sector should be tested for privacy impacts and risks prior to, and during, development and implementation. A privacy impact assessment (PIA) is a useful tool for evaluating and mitigating privacy risks.[2]

Other OAIC recommendations and policy positions

Comprehensive credit reporting

The OAIC does not support the policy proposal to expand comprehensive credit reporting by making it mandatory, adding new fields and/or extending it to SME lending. Australia's credit reporting system only recently underwent a significant process of reform and

[1] The full coverage of the *Privacy Act 1988* is outlined at: http://www.oaic.gov.au/privacy/who-is-covered-by-privacy.

[2] OAIC, *Guide to undertaking privacy impact assessments*, May 2014, http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-undertaking-privacy-impact-assessments.

should now be allowed to operate for a reasonable period of time before further assessment and change.

Regulation and technology neutrality

The OAIC supports technology neutrality in regulation – a concept embodied in the Privacy Act.

Review of new privacy requirements

The OAIC agrees that there is value in reviewing the effectiveness of the reformed Privacy Act after a reasonable period of time. However, the OAIC believes such a review will be of the greatest value if it addresses privacy requirements applying across all sectors.

Cross-border disclosure of personal information

APP 8 and s 16C of the Privacy Act establish a framework for the regulation of cross-border disclosure of personal information. This framework reflects a central object of the Privacy Act of facilitating the free flow of information across national borders while ensuring that the privacy of individuals is respected (s 2A(f)).

APP 8 and s 16C came into effect on 12 March 2014 (along with the other privacy reforms discussed above). For that reason, the OAIC suggests they be allowed to operate for a reasonable period of time before further review and assessment. Further, any review of the operation of APP 8 and s 16C should occur as part of a wider review of the new privacy requirements.

The OAIC agrees with the importance of fostering cross-border privacy enforcement cooperation and suggests that efforts to improve cross-border mutual regulatory recognition should build on the significant work of the Asia-Pacific Privacy Authorities forum, the Data Privacy Subgroup within APEC and the Global Privacy Enforcement Network (GPEN) affiliated with the OECD, and be carried forward by those networks.

Greater use of government data sets

The OAIC supports proactive publication of datasets on data.gov.au, subject to publishers complying with Privacy Act obligations and other relevant information management policies. Where an agency is considering publishing a data set with a potential privacy risk or impact, the OAIC recommends that the agency carry out a PIA and consider the OAIC's guidance on de-identification.[3]

Breach notification

The OAIC supports mandatory data breach notification and believes it should be made an element of the wider privacy regulatory framework established by the Privacy Act.

The OAIC is best placed to receive breach notifications.

[3] OAIC, *Information policy agency resource 1: De-identification of data and information*, April 2014, http://www.oaic.gov.au/information-policy/information-policy-resources/information-policy-agency-resources/information-policy-agency-resource-1-de-identification-of-data-and-information.

Cloud computing

The OAIC is aware of some uncertainty among organisations about how the APPs apply to use of cloud services and is considering whether the development of additional guidance would assist with addressing this. The OAIC suggests that it be consulted on significant new regulation or policy in relation to use of cloud computing in the financial sector.

Cyber security

The OAIC supports measures that help give organisations (including financial institutions) up-to-date information about cyber security threats. Such information would enable organisations to better meet their obligations under APP 11 — Security of personal information.

Digital identity management and authentication

The recent reforms to the Privacy Act have broadened the circumstances under which organisations are able to use government related identifiers. The OAIC suggests the Inquiry's final report could take into account this change and the resulting expansions to the Document Verification Service (DVS) in assessing the need for and shape of further changes to identity management and authentication systems in Australia.

New identity management and authentication initiatives should take account of (and build from) the substantial identity management and authentication infrastructure (including the DVS) that is already in place. They should also be subject to PIAs to identify and mitigate privacy risks.

Introduction

The Office of the Australian Information Commissioner (the OAIC) was established by the *Australian Information Commissioner Act 2010* (Cth[4]) (the AIC Act) and commenced operation on 1 November 2010.

The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner.

The Commissioners of the OAIC share two broad functions:

- the FOI functions, set out in s 8 of the AIC Act — providing access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982* (Cth), and
- the privacy functions, set out in s 9 of the AIC Act — protecting the privacy of individuals in accordance with the *Privacy Act 1988* (Cth) (the Privacy Act) and other legislation.

The Information Commissioner also has the Information Commissioner functions, set out in s 7 of the AIC Act. Those comprise strategic functions relating to information management by the Australian Government.

On 31 December 2014, in line with the Government's budget announcement in May 2014, the OAIC will be disbanded with freedom of information functions being moved to the Administrative Appeals Tribunal, the Commonwealth Ombudsman and the Attorney-General's Department. The OAIC's privacy functions will continue to be undertaken by a statutory Privacy Commissioner.[5] Throughout this submission where we have referred to the OAIC, any ongoing activity after 1 January 2015, would be carried out by the Privacy Commissioner.

[4] Including the jurisdiction may not be necessary if your audience is solely Australian Government and/or you do not refer to any State legislation in the submission.

[5] Legislation is expected to be introduced to the Australian Parliament in the spring sittings to effect these changes.

Comments on the interim report

Privacy regulation and the financial system

In Australia, handling of personal information by the financial sector is primarily regulated by the Privacy Act.

The OAIC collects and publishes statistics about its processing of privacy complaints. Preliminary figures from the 2013-14 financial year (as in 2012-13) show that the financial sector was the most complained about sector, with the OAIC receiving 1532 privacy complaints about financial and superannuation organisations. This does not necessarily indicate that the financial sector is particularly prone to mishandling customer personal information. Complaints received do not always translate into findings against the respondent organisation. Rather, it may simply signify the vast number of transactions involving personal information carried out by financial institutions on a daily basis, relative to other sectors.

Indeed, community attitudes research, commissioned by the OAIC in 2013, indicates that financial institutions enjoy a high level of trust in the community with 74 per cent of respondents saying that they thought financial institutions were trustworthy in terms of their handling of personal information.[6] This placed financial organisations second only to health service providers in the ranking of trustworthiness by organisation type.

These conditions – the high volume of personal information processed by the sector and the high level of trust in financial institutions – demand and are fostered by a strong privacy regulatory framework. In an age of online banking and digital services, now more than ever consumer confidence rests on responsible privacy practice by financial institutions.

The importance of a nationally consistent privacy law

In the OAIC's view, an important aspect of a strong and effective privacy framework is national consistency. Regulation should apply to all sectors equally, establishing uniform standards and avoiding gaps or overlap in coverage. It should also be flexible enough to cater to diverse business and technology needs and requirements. The recently reformed Privacy Act establishes such a framework. The OAIC believes the financial sector is best served by that privacy framework and we would not support measures that established differential privacy regulations for the sector, apart from measures under the Privacy Act.

The OAIC is the primary regulator for personal information handling across all large private sector organisations (including financial institutions and credit reporting bodies) and not-for-profit organisations, some smaller organisations and most Australian

[6] OAIC, *Community attitudes to privacy survey: research report 2013,* pp 27-8, http://www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013.

Government agencies.[7] The credit reporting provisions in Part IIIA apply to all credit providers regardless of their size.

Recent reforms to the Privacy Act have sought to strengthen consistency in privacy regulation. During the Australian Law Reform Commission's (ALRC) 2006-08 review of privacy law, a major issue addressed was the significant fragmentation and inconsistency in privacy regulation. In the ALRC's view:

> Inconsistency and fragmentation in privacy regulation causes a number of problems, including unjustified compliance burden and cost, impediments to information sharing and national initiatives, and confusion about who to approach to make a privacy complaint. National consistency, therefore, should be one of the goals of privacy regulation.[8]

The introduction of the Australian Privacy Principles (APPs) (following recommendations made by the ALRC) was aimed at reducing inconsistency between privacy requirements applying to the public and private sectors. In the reformed Privacy Act, a stated objective is to provide the basis for nationally consistent regulation of privacy and the handling of personal information (s 2A(c)).

In an environment where financial institutions are diversifying their operations and non-financial organisations (such as social networks and supermarkets) are moving to offer financial services, [9] it makes sense to continue to have a central rather than sector-specific approach to privacy regulation. A central privacy regime ensures uniform standards as technology changes and the traditional distinctions between sector types become blurred.

If particular privacy issues need addressing in the financial sector, an APP code would be the best option

The OAIC believes that the APPs and the credit reporting provisions in Part IIIA of the Privacy Act provide a sufficient regulatory framework for personal information handling by the financial sector. However, if the Inquiry identifies a privacy issue that warrants specific additional regulation, an APP code under the Privacy Act may be the best option. The APP code making power in the Privacy Act (Part IIIB) provides a mechanism to establish supplementary regulation where appropriate. APP codes must build on, and add specificity to, the APPs, which ensures regulatory congruity and consistency.

The OAIC is best placed to investigate alleged misuse of personal information in the financial sector and enforce privacy requirements

Essential to an effective regulatory regime is an independent regulator with powers to monitor and investigate non-compliance, and encourage best practice privacy practices.

---

[7] The full coverage of the *Privacy Act 1988* is outlined at: http://www.oaic.gov.au/privacy/who-is-covered-by-privacy

[8] ALRC, *For your information: Australian Privacy Law and Practice*, Report 108, August 2008, paragraph 3.13, http://www.alrc.gov.au/publications/report-108.

[9] See, Financial System Inquiry – Interim Report, 4-51-4-52.

The Privacy Act confers a range of regulatory action and enforcement powers on the OAIC, which are based on an escalation model. Those powers were recently expanded as part of the 12 March 2014 reforms to the Privacy Act. The powers now available to the OAIC include the power to:

- conduct an assessment of privacy compliance for both an agency and a private sector entity
- accept an enforceable undertaking and bring proceedings to enforce an undertaking
- make a determination in both a complaint investigation and a 'Commissioner initiated investigation' (CII)
- seek a civil penalty from the courts in the case of a serious or repeated interference with privacy, or in the case of a breach of certain credit reporting provisions.

While it has a range of regulatory action powers to draw on, the OAIC's preferred regulatory approach is to work with entities to encourage compliance and best practice privacy practices.[10] This approach seeks to avoid contraventions and the subsequent need to investigate matters and take formal enforcement action. Therefore, the OAIC will continue to engage with regulated entities to provide guidance, promote best practice compliance, and identify and seek to address privacy concerns as they arise.

However, where an alleged interference with privacy has occurred, the OAIC may commence an investigation, either on receipt of a complaint or as a CII. The Office generally must make a reasonable attempt to conciliate a complaint and the OAIC will resolve the majority of complaints in this way. For a CII, the OAIC generally will work with the respondent to investigate the matter. Enforcement action may then be considered following an investigation.

The OAIC's handling of privacy complaints is the final tier of a three-tiered complaint process for Privacy Act breaches. In the first instance, an aggrieved individual should complain to the respondent. Where not satisfied with the response or outcome, the individual may complain to an EDR scheme of which the respondent is a member (if any) which has been recognised by the OAIC. If the individual is dissatisfied with the outcome of the EDR process, they may complain to the OAIC and the OAIC will consider whether to accept the complaint. EDR schemes currently recognised by the OAIC include the Financial Ombudsman Service and the Credit Ombudsman Service Limited.

[10] See OAIC, *Privacy regulatory action policy (draft)*, March 2014, paragraph 22, http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/oaic-s-privacy-regulatory-action-policy/oaic-s-privacy-regulatory-action-policy-draft (the finalised policy will be published soon); see also 'The OAIC's enforcement approach to new privacy laws from 12 March 2014 — Statement from the Australian Information Commissioner and Privacy Commissioner', 28 February 2014, http://www.oaic.gov.au/news-and-events/statements/privacy-statements/oaic-enforcement-approach-to-new-privacy-laws-12-march-2014/the-oaic-s-enforcement-approach-to-new-privacy-laws-from-12-march-2014-statement-from-the-aust.

In addition to having a range of regulatory action powers to draw on, and the collaborative approach to regulation outlined above, the OAIC offers its considerable expertise and experience in privacy regulation. The OAIC also has extensive experience in complaint conciliation, meaning it provides a method for fast, informal and low-cost resolution of disputes. The inclusion of recognised EDR schemes in the OAIC's regulatory model further contributes to this efficient dispute resolution and the OAIC is committed to working collaboratively with EDR schemes to ensure consistency in the application of the APPs and credit reporting provisions.

The Privacy Act and the OAIC have high visibility in the Australian community and are regularly approached by the community about privacy concerns. This experience, expertise and visibility foster consumer confidence that privacy rights will be defended – confidence that is an indispensable part of a healthy financial system.

Comprehensive credit reporting

Interim report policy proposal:

Expand comprehensive credit reporting by making it mandatory, adding new fields and / or extending it to SME lending (2-18).

OAIC response

The OAIC does not support this policy proposal.

Australia's credit reporting system has been recently reformed

The credit reporting system in Australia has undergone a very recent reform process (which involved a move from 'negative' to more 'comprehensive' reporting and an expansion to the credit reporting fields). The new system commenced operation on 12 March 2014.

Reforms to the credit reporting system started in 2006 with a major review by the ALRC[11] and involved a rigorous development process including extensive consultation with industry and consumer representatives. That process culminated in reforms to the credit reporting provisions in the Privacy Act and the establishment of a credit reporting code of conduct.[12]

After a seven year development process, the new credit reporting system has been in place for only 5 months. In its review report, the ALRC suggested the system be reviewed 5 years after its commencement.[13] The Privacy (Credit Reporting) Code 2014 requires a review of the code to be undertaken after 3 years.[14]

[11] ALRC, *For your information: Australian Privacy Law and Practice*, Report 108, August 2008, Part G; and ALRC, *Review of Privacy – Credit reporting provisions*, Issues Paper 32, December 2006, http://www.alrc.gov.au/ip-32.

[12] OAIC, *Privacy (Credit Reporting) Code 2014 (Version 1.2)*, http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-registers/privacy-codes/privacy-credit-reporting-code-2014-version-1-2.

[13] ALRC, *For your information: Australian Privacy Law and Practice*, Report 108, August 2008, recommendation 54-8.

[14] OAIC, *Privacy (Credit Reporting) Code 2014 (Version 1.2)*, paragraph 24.3.

Making changes now would undermine the significant work that has gone into establishing the new system, including the investment by business to prepare for it. Stakeholders have had significant opportunity for input into the shape and scope of Australia's new 'comprehensive' credit reporting system. The system should now be allowed to operate for a reasonable period of time before further assessment and change, and the imposition of further costs on business.

Making participation in the system mandatory

The interim report proposes making the Australia's credit reporting system mandatory. This appears to be based on concern amongst some stakeholders about low participation in the new system by large credit providers. However, it is too early to draw conclusions about participation. The former 'negative' credit reporting system enjoyed a high level of participation by credit providers. As noted above, the new 'comprehensive' system has only recently commenced and mechanisms are still being put in place to facilitate credit provider involvement.

For example, the OAIC understands that an industry code currently under development will address this issue by establishing a framework for participation in the system based on principles of reciprocity. [15] Credit providers will be able to opt-in to the level of participation they wish and to receive a corresponding level of access to the expanded categories of information now available.

Generally, the OAIC believes the facilitation of 'tiered' access to credit reporting information by means of reciprocity may achieve better privacy outcomes, by ensuring that credit providers only gain access to particular credit reporting information of an individual that is relevant to the credit providers' particular context rather than access to all credit reporting information available.

It is likely that there will be a higher rate of participation in the credit reporting system following the commencement of the industry code. However, this may be an issue to revisit in a later review, once the system has been in operation for a reasonable period of time.

Expansion of the credit reporting system to SME lending

There are two broad credit reporting systems: one deals with consumer credit, the other with commercial credit. The credit reporting provisions in Part IIIA of the Privacy Act apply to consumer credit. The OAIC understands that SME lending is generally already the subject of credit reporting. Where a credit provider wishes to access consumer credit information about an individual seeking a small business loan, for example, the Privacy Act allows this to occur as long as the credit provider seeks the consent of the individual. Therefore, the OAIC is unclear what sort of expansion is being proposed.

[15] This code will be assessed by the Australian Competition and Consumer Commission in relation to anti-competitive issues.

Making repayment history information available to non-ASIC licenced credit providers

Some stakeholders recommend that repayment history information be made available to non-ASIC (Australian Securities and Investments Commission) licenced credit providers, such as telecommunications and utilities providers.[16]

The OAIC does not support this change. At present, only credit providers licenced by ASIC are permitted to disclose information about an individual's repayment history to a credit reporting body and access that information. Not being licenced by ASIC means that telecommunications and utilities providers are not bound by the responsible lending obligations in the *National Consumer Credit Protection Act 2009.* (Those obligations ensure that a credit provider only provides an individual with credit that is not unsuitable for them.)

While there may be some benefits to collecting more repayment history information and making it available to more types of organisations – those benefits must be weighed against the significant privacy impact on individuals. Generally, because telecommunications and utilities providers do not have responsible lending obligations, it is not necessary for them to have access to this additional information. Increasing the number of organisations with access to the information necessarily increases privacy impacts while also creating conditions for function creep, as non-financial institutions push for greater use of the information for a wider range of purposes.

As above, the OAIC suggests that, having been very recently reformed, the credit reporting system should be allowed to operate for a reasonable period before consideration of further expansions or changes.

Regulation and technology neutrality

Interim report policy proposal:

Adopt a principle of technology neutrality, for future regulation recognising the need for technology-specific regulation on an exceptions basis. Where technology-specific regulation is required, seek to be technology neutral within that class of technologies (4-44).

OAIC response

The OAIC supports technology neutrality in regulation – a concept embodied in the Privacy Act.

During its review of Australian privacy law, the ALRC considered the issue, coming to the view that 'technology-neutral privacy principles provide the most effective way to ensure individual privacy protection in light of developing technology.'[17] Principle based law also enables a degree of flexibility ensuring resilience to technology change and adaptability to diverse business needs and requirements.

[16] See Australian Retail Credit Association submission to the Financial System Inquiry, April 2014, pp 10-15.
[17] ALRC, *For your information: Australian Privacy Law and Practice*, Report 108, August 2008, paragraph 10.9.

The APPs provide a technology neutral regulatory framework for personal information handling in Australia. Further, the code making power in the Privacy Act (Part IIIB) provides a mechanism to establish supplementary technology-specific regulation where appropriate. APP codes must build on, and can add specificity to, the APPs, ensuring regulatory congruity and consistency. APP codes can be used in relation to industry sectors or the use of specific technologies.

On that basis, the OAIC believes the Privacy Act embodies the policy proposal put forward in the interim report.

Privacy and cross-border disclosure of personal information

Interim report policy proposal:

Review and assess the new privacy requirements two years after implementation to consider whether the impacts appropriately balance financial system efficiency and privacy protections (4-55).

OAIC response

The OAIC agrees that there is value in reviewing the effectiveness of reformed legislation after a reasonable period of time. However, the OAIC believes such a review will be of the greatest value if it addresses privacy requirements applying across all sectors.

National consistency of privacy regulation is desirable (see *The importance of a nationally consistent privacy law*, above). Reviewing the new privacy requirements only as they relate to the financial sector may weaken consistency by advocating for changes solely for financial institutions. As the interim report notes, financial institutions are diversifying their operations and non-financial organisations (such as social networks and supermarkets) are moving to offer financial services.[18] In this climate, where boundaries between sectors are becoming less distinct, a single central privacy regulatory framework will be critical to ensuring even coverage of business while reducing regulatory complexity for both business and consumers.

Interim report policy proposal:

Review record-keeping and privacy requirements that impact on cross-border information flows and explore options for improving cross-border mutual regulatory recognition (4-55).

OAIC response

Cross-border information flows are regulated by APP 8 and s 16C of the Privacy Act. APP 8 and s 16C establish a framework for the regulation of cross-border disclosure of personal information. This framework generally requires an APP entity to take reasonable steps to ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information (subject to some exceptions). This reflects a central object of the Privacy Act, of facilitating the free flow of information across national

[18] See, Financial System Inquiry – Interim Report, 4-51-4-52.

borders while ensuring that the privacy of individuals is respected (s 2A(f)).[19] It also reflects the accountability principle contained in the APEC Privacy Framework.[20]

APP 8 and s 16C only came into effect on 12 March 2014 (along with the other privacy reforms discussed above). For that reason, OAIC suggests they be allowed to operate for a reasonable period of time before further review and assessment. Further, any review of the operation of APP 8 and s 16C should occur as part of a wider review of the new privacy requirements.

The OAIC is involved in a range of initiatives aimed at strengthening cross-border cooperation on privacy enforcement, including through the Asia-Pacific Privacy Authorities (APPA) forum[21] the Data Privacy Subgroup within APEC[22] and the Global Privacy Enforcement Network (GPEN) affiliated with the OECD.[23] Much effort has been invested in addressing the challenge of personal information moving easily between recipients, irrespective of borders and legal jurisdictions. Cross-border cooperation on privacy enforcement has been recognised as a critical goal both to facilitating free flow of information (and thus fostering the digital economy) and ensuring consumer confidence and protection of privacy. Therefore, both APEC and OECD (through GPEN) have developed or are developing frameworks that support cooperation on privacy enforcement.[24]

The OAIC has outlined how it will cooperate with overseas privacy enforcement authorities in its draft *Privacy regulatory action policy.* In the policy, OAIC commits to working in partnership with privacy regulators in foreign jurisdictions where the OAIC's interests in protecting personal information align with the interests of other regulators. Through those partnerships, the OAIC states that it will share knowledge and expertise with a view to ensuring a consistent and harmonised approach to regulatory action in a particular matter. If appropriate, the OAIC may also seek to coordinate regulatory activities and share investigative information with foreign privacy regulators. However, the OAIC will always operate within its legislative framework, including limits on its ability to share information.[25]

---

[19] See OAIC, *Australian Privacy Principles Guidelines,* Chapter 8: APP 8 – Cross-border disclosure of personal information, February 2014, 8.1, http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information.

[20] See APEC Privacy Framework, 2005, Principle 9, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

[21] http://www.appaforum.org/.

[22] See the Data Privacy Subgroup within the Electronic Commerce Steering Group, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx which advances the objects of the APEC Privacy Framework, http://publications.apec.org/publication-detail.php?pub_id=390.

[23] Global Privacy Enforcement Network, https://www.privacyenforcement.net/.

[24] See APEC, *Cross-border Privacy Enforcement Arrangement*, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx; and OECD, *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, http://www.oecd.org/internet/ieconomy/oecdrecommendationoncross-borderco-operationintheenforcementoflawsprotectingprivacy.htm/.

[25] OAIC, *Privacy regulatory action policy (draft)*, March 2014, paragraph 47.

The OAIC suggests that efforts to improve cross-border mutual regulatory recognition should build on the significant work of the networks outlined above, and be carried forward by those networks.

Interim report question:

What options could be explored for providing consumers with more control over use of their data and / or better access to their own data in useful formats to improve decision making and consumer outcomes? (4-55)

OAIC response

The OAIC supports greater ease of access for consumers to their personal information. This would advance the objectives of APP 12 which establishes minimum standards for access by individuals to their personal information held by organisations and agencies.

Greater use of government data sets

Interim report question:

What additional Government data sets could be released to improve consumer outcomes, industry analysis and public policy development via data.gov.au, taking into account relevant privacy requirements? (4-55)

OAIC response

The OAIC supports proactive publication of datasets on data.gov.au, subject to publishers complying with Privacy Act obligations and abiding by appropriate information management policies including the *Principles on open public sector information*[26] and de-identification guidance[27] issued by the OAIC. Publishers should also give regard to the *Open data toolkit* which is currently under development and is available at https://toolkit.data.gov.au).

Where an agency is considering publishing a data set with a potential privacy risk or impact, the OAIC recommends that the agency carry out a privacy impact assessment (PIA). A PIA is an assessment tool that allows entities to assess the privacy impact of new initiatives, test compliance with privacy law and identify effective ways to mitigate privacy risks. A guide to undertaking PIAs is available on the OAIC's website.[28]

[26] OAIC, *Principles on open public sector information*, May 2011, http://www.oaic.gov.au/information-policy/information-policy-resources/information-policy-agency-resources/principles-on-open-public-sector-information.

[27] OAIC, *Information policy agency resource 1: De-identification of data and information*, April 2014, http://www.oaic.gov.au/information-policy/information-policy-resources/information-policy-agency-resources/information-policy-agency-resource-1-de-identification-of-data-and-information.

[28] OAIC, *Guide to undertaking privacy impact assessments*, May 2014, http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-undertaking-privacy-impact-assessments.

Mandatory data breach notification

Interim report policy proposal

Implement mandatory data breach notifications to affected individuals and the Australian Government agency with relevant responsibility under privacy laws (4-58).

OAIC response

The OAIC supports mandatory data breach notification.

Existing voluntary framework for breach notification

The interim report cites the OAIC's Data Breach Notification Guide. The guide establishes a framework for dealing with data breaches and, where relevant, the voluntary notification of breaches to the OAIC. Preliminary figures for the 2013–14 financial year, show the OAIC received 72 voluntary breach notifications, an 18% increase on the number of notifications received in 2012–13. Reports of current breach activity, such as Symantec's 2014 *Internet Security Threat Report,* indicate that voluntary notifications received by the OAIC are likely to account for only a portion of the breaches potentially affecting Australians.[29]

Currently there is no specific obligation to report breaches, other than the mandatory scheme under s 75 of the *Personally Controlled Electronic Health Records Act 2012*. However, many agencies and organisations choose to do so as good privacy practice and as part of taking reasonable security steps. The OAIC's response to notifications primarily focuses on the data security measures that the entity had in place when the incident occurred and the steps taken to improve security practices in future to achieve the best privacy outcome for affected individuals. The OAIC may take no further action if it considers that the reporting entity had taken appropriate steps to respond to the data breach, including mitigating harm to affected individuals.

In cases where the OAIC is not satisfied with the voluntary action taken by the agency or organisation to resolve the matter, or where the nature of the breach warrants further action, a Commissioner-initiated investigation may be opened.

Ensuring breach notification is part of a cohesive privacy regulatory framework

The OAIC believes it is appropriate that mandatory breach notification be made an element of the wider privacy regulatory framework established by the Privacy Act. This fosters a continuity of regulatory coverage and action. Breaches notified under the Privacy Act would be able to be investigated by the OAIC (where appropriate) using the enforcement powers available under the Privacy Act and the incident would be measured against the standards set out in the APPs.

The OAIC is best placed to receive breach notifications as it has wide experience under the existing voluntary scheme, and the mandatory scheme under s 75 of the *Personally*

[29] Symantec, *2014 Internet Security Threat Report,* volume 19, http://www.symantec.com/security_response/publications/threatreport.jsp.

Controlled Electronic Health Records Act 2012, and the requisite enforcement powers to ensure that serious breaches are appropriately investigated.

Cloud technology

Interim report policy proposal:

Communicate to APRA continuing industry support for a principles-based approach to setting cloud computing requirements and the need to consider the benefits of the technology as well as the risks (4-58).

OAIC response

The OAIC supports principles-based regulation of personal information handling. As discussed above, the APPs are technology neutral and therefore will equally apply to an APP entity's use of cloud computing services where these are employed to collect, use, disclose and/or store personal information.

A clear benefit of a principles-based approach is that the OAIC can monitor emerging trends, and develop guidance outlining how the principles might practically apply to personal information handled through use of a particular technology. The OAIC has published non-binding guidance to assist with interpreting the APPs (the APP guidelines).[30] These guidelines include examples of how the APPs may apply to personal information handled in the cloud.

The APP guidelines make clear that the APPs do not prevent APP entities from using services offered by Australian or overseas cloud vendors. However, before contracting with a cloud service provider, APP entities will need to take account of their responsibilities under the Privacy Act. This includes ensuring, where required, that appropriate privacy protections apply to personal information in the cloud, before the information is given to a cloud service provider. The entity should also be aware that it may be held accountable under the Privacy Act, for mishandling of the information by an overseas cloud service provider.

Privacy risks associated with cloud computing

The interim report outlines some of the risks associated with cloud computing, particularly the way that it '…potentially dilutes a firm's control over its data and systems, increasing security risks.'[31] The Department of Communications recent *Cloud Computing Regulatory Stock Take* also identified a range of privacy risks and considerations.[32] These include entities having difficulties assuring themselves that data is being stored securely and destroyed or de-identified in line with APP 11 obligations; risks of data loss where a cloud service provider abruptly ceases operation; personal information being stored in overseas jurisdictions subject to different, potentially more privacy intrusive or less

[30] Available at http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/.
[31] Financial System Inquiry – Interim Report, 4-57.
[32] See Department of Communications, *Cloud Computing Regulatory Stock Take*, May 2014, Chapter 3, http://www.communications.gov.au/digital_economy/cloud_computing.

privacy protective legislation; and generally deficient contractual arrangements between entities and cloud service providers.

The OAIC is aware of privacy risks associated with cloud computing (including those outlined above). It also understands that there are a range of benefits associated with use of cloud services. Given these factors, as well as the considerable community discussion of cloud computing issues, the OAIC is considering whether additional guidance either in the APP guidelines or in agency or business resources would assist.

We suggest that the OAIC be consulted on significant new regulation or policy in relation to use of cloud computing in the financial sector.

Cyber security

Interim report policy proposal:

Review and update the 2009 Cyber Security Strategy to reflect changes in the threat environment, improve cohesion in policy implementation and progress public-private sector collaboration (4-63).

OAIC response:

The OAIC supports measures that help give organisations (including financial institutions) up-to-date information about cyber security threats. Such information would enable organisations to better meet their obligations under APP 11. APP 11 requires entities to take such steps as are reasonable in the circumstances to protect personal information they hold from misuse and unauthorised access, modification or disclosure. What steps are reasonable depend on the circumstances and may include any known or potential cyber security threats at a given time.

Digital identity management and authentication

Interim report policy proposal:

Develop a national strategy for promoting trusted digital identities, in consultation with financial institutions and other stakeholders (4-70).

Interim report questions:

In developing a national strategy, what should be the respective roles, responsibilities and expectations of Australian public and private sector organisations in creating, accepting and maintaining the digital identities used by Australians? (4-71)

Is there a need for Government to enhance identity authentication by facilitating interoperability standards in areas such as biometrics, enabling better access to Government information or improvements to the Document Verification Service? (4-71)

OAIC response

Recent changes to identity management and authentication following reforms to the Privacy Act

The recent reforms to the Privacy Act have broadened the circumstances under which organisations are able to use or disclose government related identifiers.

In addition to other exceptions, an organisation may now use or disclose a government related identifier where it is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions (APP 9.2(a)).

This change has enabled an expansion of Document Verification Service (DVS) users to include private sector organisations, where previously the DVS was only available to government agencies. This is a significant change for the DVS. Additional expansions to the DVS are also under consideration, including expansion of access to the DVS amongst government and private sector organisations in Australia and New Zealand that meet the necessary requirements of the *Privacy Act 1998.*[33] The Inquiry's final report should take into account recent and proposed expansions to the DVS in assessing the need for and shape of further changes to identity management and authentication systems in Australia.

The interim report notes the many other initiatives in Australia currently in operation or under development, including the National Identity Security Strategy, the Third Party Identity Services Assurance Framework; the National e-Authentication Framework; the National Identity Proofing Guidelines and the myGov service (see for example 4-66). Any new initiatives should take account of (and build from) the substantial identity management and authentication infrastructure (including the DVS) that is already in place.

Ensuring careful consideration of privacy in new identity management systems

Digital identity management and authentication should involve careful consideration of privacy issues. During the development of new identity management and authentication systems or changes to existing systems, PIAs should be carried out to identify and mitigate privacy risks. A PIA will also help to ensure that identity management and authentication systems comply with the Privacy Act.

Generally, good identity management and authentication should avoid:

- collecting more information than is necessary
- storing more information than is necessary
- creating a de facto ID card or number through which all of a person's information can be easily linked, matched or mined across all facets of the person's life

[33] See the Communique from the Council of Australian Governments' Law, Crime, and Community Safety Council meeting held in July 2014: http://www.lccsc.gov.au/sclj/lccsc_communiques/2014_communiques.html

- establishing a centralised database of personal information attractive to hackers and ID thieves
- removing an individual's choice over when and to what extent they identify themselves to someone else.

The OAIC was consulted during the development of many of the identity management and authentication projects and initiatives outlined above and should be consulted on new initiatives to develop or change identity management and authentication in Australia.