Australian Government
Office of the Australian Information Commissioner

Submission on the Financial System Inquiry Final Report

Submission to the Treasury

April 2015

Timothy Pilgrim, Australian Privacy Commissioner

Contents

The Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner (OAIC) is an independent statutory agency within the Attorney General's portfolio, with functions that include independent oversight of privacy protections in the *Privacy Act 1988* (Cth) (Privacy Act). The Privacy Act confers a range of functions on the Australian Information Commissioner which are also conferred on the Privacy Commissioner by operation of the *Australian Information Commissioner Act 2010* (Cth).[1]

General Comments

1. The OAIC welcomes the opportunity to provide the Treasury with comments on the Financial System Inquiry Final Report (the Report), which supplement the comments made in the OAIC's Submission on the Inquiry's Interim Report.
2. The Report makes a number of recommendations that relate to privacy, most of which are contained in 'Chapter 3: Innovation'. Accordingly, the OAIC has largely limited its comments to the recommendations made in that chapter, specifically:
    - Recommendation 14: Collaborate to enable innovation
    - Recommendation 15: Digital identity
    - Recommendation 19: Data access and use
    - Recommendation 20: Comprehensive credit reporting.
3. In making the comments below, the OAIC recognises the benefits that technology-driven innovation can bring to the financial services industry, including through the development of new products and services, new business models, increased competition and improved customer service and convenience. However, to the extent that these new technologies involve the handling of personal information, it is important to ensure that they are accompanied by the necessary privacy protections.
4. In Australia the handling of personal information is primarily regulated by the Privacy Act. The Privacy Act contains the 13 Australian Privacy Principles (APPs), which apply to most Australian and Norfolk Island government agencies and private sector organisations with an annual turnover of more than $3 million (called 'APP entities'). The APPs are designed to ensure that individuals' personal information is protected throughout the information lifecycle – that is, from the time the information is collected through to its destruction. The APPs also give individuals the right to access their personal information and have it corrected if it is incorrect. For more information about the APPs please see the OAIC's APP Guidelines.
5. Additionally, Part IIIA of the Privacy Act and the *Privacy (Credit Reporting) Code 2014* together regulate consumer credit reporting in Australia (hereinafter, referred to as the Australian consumer credit reporting laws). All Australian credit reporting bodies and credit providers are required to comply with those laws when handling types of

[1] See s 12 of the *Australian Information Commissioner Act* 2010.

personal information made available through the Australian credit reporting system. For more information about the Australian credit reporting laws please see the OAIC's credit reporting 'know your rights' series of fact sheets.

6. Accordingly, the Privacy Act provides the central framework for regulating the handling of personal information by APP entities, including the financial sector. In that respect, the OAIC takes this opportunity to reiterate the view expressed in its submission on the Interim Report, that the Privacy Act should remain the central framework for regulating the handing of personal information within the financial sector. The OAIC considers that the Privacy Act is well-adapted to ensuring the protection of individual privacy in an environment of technology-driven innovation for the following reasons:

   - the APPs are principle-based, thereby providing entities with the flexibility to tailor their personal information handling practices to their needs and business models, and to the needs of individuals (in this way the APPs also ensure competitive neutrality in privacy regulation)
   - the APPs are technology neutral, thereby ensuring that they remain applicable in the face of continually changing and emerging technologies
   - the Privacy Act provides entities with the ability to make a binding code where greater particularity about how the APPs should be implemented in relation to a particular sector or technology is desirable (see s 26 of the Privacy Act), and
   - the Privacy Act is the privacy oversight instrument with which the public is most familiar and, therefore, reflects community expectations of the appropriate level of protection that should be afforded to personal information in Australia.

Specific Comments

A. Recommendation 14: Collaborate to enable innovation

7. The Report recommends the establishment of a public-private collaborative committee (the 'Innovation Collaboration') to facilitate financial system innovation and to enable timely and coordinated policy and regulatory responses.[2]

8. The OAIC recognises that collaboration between industry, regulators, consumer groups and other stakeholders is important to help facilitate innovation and ensure that regulatory responses to innovation within the financial sector are both informed and consistent. This type of collaboration is particularly important in the context of privacy regulation which applies uniformly across all Australian industries. The disparate nature of the entities that operate in those industries means that appropriate collaboration can help inform the OAIC's policy and regulatory approach.

9. The importance of working with regulated entities is also embedded in the OAIC's regulatory approach to privacy, as outlined in the Office's Privacy regulatory action

[2] See the Financial System Inquiry Final Report (the Report), p 147.

policy (the Policy). The Policy explains that the OAIC's preferred regulatory approach is to facilitate voluntary compliance with privacy obligations and to work with entities to create a culture of privacy compliance by embedding good privacy practice into business processes and, thereby, prevent privacy breaches. The OAIC considers that this approach to using its regulatory powers under the Privacy Act is also the approach most conducive to facilitate innovation.

10. With this in mind, the OAIC welcomes the proposal to create the Innovation Collaboration. The OAIC considers that this new channel of communication will assist regulators to stay abreast of technological developments in the financial services industry, including developments that involve the handling of personal information. At the same time, the Innovation Collaboration could also provide a new channel to assist industry to understand their obligations under the Privacy Act. This has the added benefit of assisting innovators to identify any privacy impacts at the design stage of developing new financial products and services, which will allow them to build- the necessary privacy protections into new products or services to mitigate these impacts (known as 'privacy by design').

11. While the OAIC is not in a position to be a permanent participant in the Innovation Collaboration, the OAIC would welcome engagement with the committee in relation to particular initiatives that raises privacy issues.

B. Recommendation 15: Digital identity

12. The Report recommends the development of a national strategy for a federated-style model of trusted digital identities in which public and private sector identity providers would compete to provide trusted digital identities to individuals and businesses.[3]

13. The OAIC recognises the benefits, both for the financial sector and individuals, of having a robust and efficient digital identity management system in Australia. Further, that such a system, if implemented correctly, can enhance privacy protections for individuals. In that respect, the OAIC supports the recommendation in the Report that any model of trusted digital identities that is developed should be transparent and privacy enhancing.[4]

14. Consistent with the OAIC's comments in its Submission on the Interim Report, the OAIC considers that a privacy enhancing identity management model should:

    - ensure that only the minimum amount of personal information necessary to identify the individual is collected – noting that the amount and type of personal information required may vary depending on the specific circumstances
    - ensure that new entrants into any market for identity services understand their obligations under the Privacy Act when handling individuals' personal information

[3] See the Report, p 151.
[4] See the Report, p 151.

- ensure that each identity credential or service provider (public or private) handles personal information in a way that is consistent with the privacy expectations of Australians, as reflected in the standards set by the APPs.
- avoid creating a centralised database or databases that might be an attractive target for hackers
- avoid creating a de-facto identity 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, and
- encourage a privacy impact assessment (PIA) to be undertaken and published in relation to new identity credentials or services (discussed further below).

15. The Report also states that the model should be 'voluntary and enable consumer choice and convenience'. The Privacy Act is premised on individuals being able to make an informed choice about whether to provide personal information to an entity. In the context of identity management, this means ensuring that the individual understands why they are being asked to provide the personal information to identify themselves and the consequences if they choose not to provide it (consistent with the notice requirements in APP 5). The OAIC therefore supports the Report's emphasis on voluntariness in the context of any digital identity management system.

Privacy impact assessments

16. A PIA is a useful tool that can assist entities to highlight any likely privacy impacts associated with policy proposals, such a federated model of digital identities, and ways to eliminate or mitigate those impacts. In addition, publishing a PIA can help to foster and maintain public confidence and trust in any digital identity model by reassuring the public that privacy is being considered and that appropriate privacy safeguards are being built-in.

17. Accordingly, the OAIC recommends that a PIA be undertaken during the design stage of any model for managing digital identity in Australia. That PIA should consider, among other things, the likely privacy impacts of creating a market for identity services and how to minimise those impacts. In addition, the OAIC recommends that a PIA be undertaken by any future identity credential or service providers seeking to enter such a market. Information about how to conduct a PIA can be found in the OAIC's Guide to undertaking privacy impact assessments, available on the OAIC website www.oaic.gov.au.

Creation of a public-private sector task force

18. The Report also recommends the creation of a public-private sector taskforce to inform the development of any digital identity model.

19. As outlined in the Report, Australia already has a number of identity initiatives in place which could form part of any federated digital identity model. The OAIC participates in various forums relating to identity management and, through these forums, it has been consulted and has provided input in relation to many of those initiatives, including:

- the Document Verification Service (DVS)
- myGov digital credentials
- the National Identity Proofing Guidelines, and
- the Third Party Identity Service Providers Assurance Framework.

20. While the OAIC is not in a position to be a permanent member of any public-private task force, the OAIC would welcome the opportunity to assist the task-force in considering how to manage any privacy impacts related to the model.

C. Recommendation 19: Data access and use

21. The Report recommends that the Government commission the Productivity Commission to commence an inquiry into the costs and benefits of increasing access to and improving the use of data, subject to privacy considerations (the Inquiry).[5]

22. The OAIC acknowledges the potential benefits to both the financial sector and consumers from increased access to and use of data. However, where that data is also personal information it has the potential to adversely impact on individuals' privacy interests if it is not accompanied by the appropriate level of privacy safeguards. With that in mind, the OAIC welcomes the emphasis that the Report places on the need for the Inquiry to consider any likely privacy risks and appropriate privacy protections.

23. As discussed above, the Privacy Act provides the central framework for regulating the handling of personal information by APP entities, including those entities in the financial sector, for which the Privacy Commissioner has regulatory oversight. Accordingly, the OAIC suggests that the Productivity Commission consult with the Privacy Commissioner in relation to matters considered in the Productivity Commission's inquiry that raise privacy issues. The OAIC can also provide the Productivity Commission with any other information about entities' obligations under the Privacy Act that the Commission might find useful.

24. In that respect, the OAIC notes that the Report lists a range of matters that the Inquiry should consider, a number of which are likely to raise privacy issues. The comments below address each of these matters separately.

Further amendments to the Privacy Act 1988

25. The Report recommends that that the Productivity Commission should consider and report to the Treasurer on potential amendments to the Privacy Act, with the intention that those amendments could be considered as part of the broader post implementation review of the reforms to that Act, which took effect on 12 March 2014.

26. The OAIC notes that the reforms to the Privacy Act, which included the introduction of the APPs, were the culmination of a law reform process which began in 2004, and which included a major review by the Australian Law Reform Commission (ALRC)

[5] See the Report, p 181.

into the protection of privacy in Australia.[6] Further, that throughout the law reform process there was extensive public consultation undertaken on the Privacy Act and the APPs in particular. Given that those reforms have only been in operation for little over a year, the OAIC considers that this is not a sufficient amount of time to enable the Productivity Commission to undertake an evaluation of the effectiveness of the new requirements, and whether any further amendments are required.

Facilitating individuals' access to their personal information

27. The Report recommends that that the inquiry should consider mechanisms to improve individuals' access to public and private sector data about themselves.

28. As noted in the Report, APP 12 provides a framework for giving individuals access to their personal information. Under APP 12, an APP entity that holds personal information about an individual must, on request, give that individual access to the information (subject to limited exceptions). Importantly, APP 12 only sets out the *minimum* access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused. APP 12 operates alongside, and does not replace, other informal or legal procedures by which an individual can be given access to information.

29. However, the OAIC acknowledges the concern expressed in the Report that the following impediments are still preventing consumers from being able to use their personal information effectively, namely that:

    - little guidance is available on how personal information should be provided
    - in most cases, consumers are unable to authorise trusted third parties to access their personal information directly from their service provider, and
    - confusion exists over what constitutes personal information.

30. In relation to the first concern, the OAIC notes that Chapter 12 of the APP Guidelines provides some guidance about how access is to be given under APP 12. However, as the APPs only set out minimum requirements and apply across all Australian industries, that guidance is general in nature, rather than being specific to the financial sector. This means that it is open to entities to adopt processes and procedures that make it easier for individuals to access their personal information, which is something that the OAIC both encourages and supports. The OAIC encourages entities, to endeavour to provide access in a manner that is as prompt, uncomplicated and inexpensive as possible[7].

31. In addition to the OAIC guidance on APP 12, there are mechanisms in the Privacy Act that allow for entities to develop binding obligations that apply in addition to those in the APPs. Under the Privacy Act, an APP entity (or a body or association representing them) can develop a written code of practice for the handling of

[6] See Office of the Australian Information Commissioner (OAIC), Privacy law reform webpage, available online : http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform

[7] See OAIC, APP 12 — Access to personal information , (2014), paragraph 12.19, available online: http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-12-app-12-access-to-personal-information

personal information, called an APP code. An APP code sets out how one or more of the APPs are to be applied or complied with, and the APP entities that are bound by the code. Once registered, a breach of a registered code will be an interference with the privacy of an individual under s 13 of the Privacy Act. Accordingly, APP entities operating within the financial sector may wish to consider developing an APP code setting out further details of how individuals' are to be provided with access to their personal information under APP 12. For more information about APP codes, please see the OAIC's Guidelines for developing codes.

32. In relation to the second concern, the OAIC notes that the Privacy Act does not prevent an individual from authorising a third party to access their personal information on their behalf, other than certain entities being excluded from accessing credit reporting information on behalf of an individual (see s 20R(2) and 21T(2) of the Privacy Act, and the definition of access seeker in s 6L of the Privacy Act). For more information about providing access to third parties, please see paragraphs 12.15 to 12.17 of Chapter 12 of the APP Guidelines.

33. In relation to the third concern, the OAIC has published some guidance about the meaning of personal information in Chapter B of the APP Guidelines and will also look to developing further guidance in the future. However, the OAIC would suggest that where entities are unsure whether particular information is personal information, they should take a risk based approach and treat the information as personal information.

Access to private sector data

34. The Report recommends that the inquiry consider mechanisms to increase access to private sector data, including through data-sharing arrangements.

35. The OAIC notes that where private sector data is also personal information, increasing access to that data has implications for individuals' privacy. Therefore, it is important that any initiatives to increase access to private sector data consider the likely privacy impacts and put in place measures to eliminate or reduce those impacts. For example, by conducting a PIA (discussed above) in the design stages of any proposed mechanisms for increasing access to data, and by ensuring that the information is appropriately de-identified where possible[8].

Engendering consumer confidence and trust

36. The Report recommends that the inquiry consider mechanisms to enhance and maintain individuals' confidence and trust in the way data is used. Expanding on this, the Report identifies the need for financial service providers to be transparent about their information management practices in order to ensure that individuals understand how their personal information is handled.

37. Relevantly, APP 1 imposes obligations on APP entities which are intended to ensure that they manage personal information in an open and transparent way. This includes an obligation to:

[8] See OAIC Privacy Business Resource 4 - de-identification of data and information, (2014), available online: http://www.oaic.gov.au/privacy/privacy-resources/privacy-business-resources/privacy-business-resource-4-de-identification-of-data-and-information

- take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints, and
- have a clearly expressed and up-to-date APP privacy policy about how the entity manages personal information.

38. Importantly, an APP privacy policy is not just a legal requirement, but is also a tool that organisations can use to generate trust by helping customers understand how the organisation handles their personal information. For more information about APP privacy policies please see the OAIC's Guide to developing an APP privacy policy guidance[9].

D. Recommendation 20: Comprehensive credit reporting

39. The Report recommends that the Government should support industry efforts to expand credit data sharing under the new voluntary comprehensive credit reporting regime. Further, that if over time participation in the credit reporting system is inadequate, the Government should consider legislating mandatory participation. The Report also suggests that the Government could consider expanding comprehensive credit reporting to include more data fields, such as the balance on an individual's consumer credit account.[10]

40. As explained above, Australia's consumer credit reporting laws are contained in the new Part IIIA of the Privacy Act and the *Privacy (Credit Reporting) Code 2014*, which were introduced as part of the reforms to the Privacy Act. Those laws set out an exhaustive list of the types of information that may be collected by a credit reporting body for inclusion in individuals' consumer credit report, as well as the entities that can access those reports. As part of its privacy functions, the OAIC is responsible for overseeing entities' compliance with those laws.

41. With that in mind, the comments below address the two elements of Recommendation 20 separately.

Expansion in the types of information permitted in the Australian consumer credit reporting system

42. The OAIC reiterates the comments made above, that Australia's new consumer credit reporting laws were the product of a lengthy reform process and extensive public consultation. Like the APPs, those laws commenced last year, on 12 March 2014.

43. That reform process included a detailed review of the types of information that should be permitted to be made available through the Australian consumer credit reporting system. The OAIC notes that the ALRC specifically considered whether information about the balance of an individual's credit account should be permitted to be included on an individual's consumer credit report. The ALRC concluded that

[9] See OAIC, *Guide to undertaking privacy impact assessments*, (2014), available online: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-developing-an-app-privacy-policy

[10] See the Report, p 190.

while certain information about an individual's repayment history should be allowed in the system, the prohibition on the reporting of current account balances should be retained.[11] Further, the OAIC notes that this recommendation was accepted by the Government in its first stage response to the ALRC Report.[12]

44. The OAIC is of the view that any consideration of an expansion in the types of information permitted to be handled in the credit reporting system is premature because (as acknowledged in the Report) industry has not begun exchanging the new types of information that were introduced as part of the shift to more comprehensive credit reporting on 12 March 2014. In that respect, the OAIC notes that the Government, in its first stage response to the ALRC Report 108, accepted the ALRC's recommendation that the new credit reporting laws should be reviewed after 5 years from the date of commencement.[13]

45. The OAIC suggests that it would be more appropriate to consider the issue of expanding the types of information permitted in the Australian consumer credit reporting system during that review.

Mandating participation in the Australian consumer credit reporting system

46. In relation to the Report's consideration of ensuring adequate participation in the Australian credit reporting system, the OAIC notes the Australian Retail Credit Association has developed an Industry Code (called the 'Principles of Reciprocity and Data Exchange') that would establish a system for the exchange of consumer credit information between credit reporting bodies and signatory credit providers. That industry code is currently being considered by the ACCC.

47. The OAIC notes that the introduction of the Principles of Reciprocity and Data Exchange may add weight to the perceived net benefits that the credit reporting system has for credit providers, which was identified in the Report as a key consideration for the level of participation in the system. As such, this may create a natural increase in participation of the system by credit providers, without the need to mandate participation in the system.

48. The OAIC also notes the additional regulatory and compliance burden that would be placed on smaller entities that are captured under the definition of a credit provider in the Privacy Act, if they are mandatorily required to participate in the consumer credit reporting system.

49. As such, the OAIC believes that it would be premature, at this stage, to consider mandating participation in the credit reporting system. Instead, this may also be considered as part of the review of the credit reporting laws, discussed above.

---

[11] See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008), page 1841, available online: http://www.alrc.gov.au/publications/55 %20More%20Comprehensive%20Credit%20Reporting/models-more-comprehensive-credit-reporting

[12] See Enhancing National Privacy Protection—Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice, (Australian Government First Stage Response), (2009), Recommendation 55-4

[13] See Australian Government First Stage Response, Recommendation 54-8