Australian Government
Office of the Australian Information Commissioner

www.oaic.gov.au
GPO Box 5218 Sydney NSW 2001
P +61 2 9284 9800 F +61 2 9284 9666
E enquiries@oaic.gov.au
Enquiries 1300 363 992 TTY 1800 620 241
ABN 85 249 230 937

Our reference: D2017/006095

Open Banking Review Secretariat
The Treasury
Langton Crescent
PARKES ACT 2600

Dear Secretariat

Submission on Issues Paper - Review into Open Banking in Australia

I welcome the opportunity to provide comments on the Issues Paper for the *Review into Open Banking in Australia*.

The Issues Paper outlines the context and background for the Government's decision to introduce an Open Banking Regime, and invites submissions on the most appropriate model for the Australian context and how best to implement this. In this regard, the Issues Paper invites submissions to address, among other things:

- what data should be shared, with whom, and how
- how to ensure that data is kept secure and privacy is respected, and
- what regulatory framework is needed to implement the regime.

By way of an overall comment, I am strongly supportive of initiatives which seek to give individuals greater choice and control over how their data is used. I also acknowledge the important policy objectives of the Review (as reflected in the Issues Paper), which include ensuring that individuals can use their data to enable the provision of new or better financial services, to increase competition, and to drive innovation.

An Open Banking regime would have significant implications for the handling of individuals' personal information that will need to be considered when designing an appropriate model. In particular, I note that 'banking data' constitutes 'personal information' as defined in section 6 of the *Privacy Act 1988* (Cth) (Privacy Act).[1]

In order to assist the work of the Review, in this submission I have outlined the responsibilities of my Office and how access to banking data is currently regulated under the Privacy Act. I also make two recommendations. First, that any new Open Banking regime should build on the existing Privacy Act framework, and second that a privacy impact

[1] The only exception may be small business banking data, which may not constitute personal information where it is about a business and not an identifiable or reasonably identifiable individual.

assessment should be conducted for any new proposals. Given the extent of the potential overlap between an Open Banking regime and the regulation of banking data under the Privacy Act, I would appreciate the opportunity to engage further with the Treasury in relation to any new policy proposals as these are developed.

About the Office of the Australian Information Commissioner (OAIC)

The Australian Parliament established the OAIC in 2010 to bring together three functions:

- freedom of information functions (access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982* (Cth)
- privacy functions (regulating the handling of personal information under the Privacy Act, and other Acts), and
- information management functions.

Together, in the exercise of these three functions the OAIC has acted in the various roles of regulator, decision maker, adviser, researcher and educator to individuals, businesses and agencies alike.

In this regard, my Office has produced a comprehensive suite of guidance to assist organisations to comply with the Australian Privacy Principles (APPs), which set out the standards that apply to the collection, use, disclosure, storage, management and other handling of personal information. Such guidance has included the *APP Guidelines*,[2] which provide comprehensive advice on all aspects of the application of the APPs, and the *Guide to securing personal information*,[3] which provides organisations with advice on how to take 'reasonable steps' to comply with APP 11 and protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure.

At the same time, in the exercise of its strategic information and freedom of information policy functions, the OAIC has worked to ensure public sector information is made available to the community as openly as possible. The OAIC's work in this area has provided an opportunity not only to reiterate core FOI and privacy themes, but to connect and unify them in a broader policy setting focussed on responsible information management. Over the last seven years the OAIC has therefore worked to encourage an 'open access by default' approach to government information, for example through the development of the *Principles on open public sector information*.[4]

The integration of these three interrelated functions into one agency has therefore meant the OAIC is well placed to strike the right balance between confidentiality and transparency — between the right to privacy, and the right to access information, which should be recognised as a key national resource. It has also provided my Office with a unique insight into many of the issues canvassed by the Issues Paper, on potential means of improving the ability of

---

[2] Available on the OAIC's website.

[3] Available on the OAICs website.

[4] Available on the OAIC's website.

individuals to make better use of their banking data (while ensuring appropriate safeguards are in place).

The regulation of banking data under the Privacy Act

As the Issues Paper outlines, an Open Banking regime would aim to give individuals greater access to and control over their own banking data, by allowing them to direct that they (or third parties) be provided with certain parts of their banking data in accordance with an established process. Whatever specific types of banking data are ultimately included in the scope of the new regime, it is important to bear in mind that these will all constitute personal information for the purposes of the Privacy Act where they are about an identifiable (or reasonably identifiable) individual.

Personal information

Personal information is defined in section 6 of the Privacy Act as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable' (regardless of whether it is true, or recorded in a material form). Personal information encompasses a broad range of information. For further information on the meaning of personal information, see the guidance sheet entitled '*What is personal information*?', recently published by my Office.

As outlined above, banking data - being information about an individual's banking and financial services and/or history - constitutes personal information. It is therefore subject to the regulatory standards set out in the Australian Privacy Principles (APPs) in Schedule 1 to the Privacy Act. The APPs govern how private sector organisations (including banks and other financial institutions)[5] may collect, use, disclose and store information about their customers, and the circumstances in which individuals may access, correct and/or transfer their banking data.

APP 12 gives individuals the ability to access and receive a copy of the personal information held about them by their financial institution, subject to some exceptions.[6] Importantly, the categories of information which individuals currently have a right to access under APP 12 is potentially broader than the categories of 'banking data' that may be covered by an Open Banking regime.

APP 12 prevents organisations from imposing a charge solely for the making of an application to access personal information. Further, any fees charged by an organisation in relation to the actual provision of access 'must not be excessive'.[7] Individuals can also request that their information be provided in a particular form, for example, in an electronic or machine-readable form, or in an accessible form for those with a visual or hearing impairment. Finally, the APPs do not prevent individuals from requesting access to their personal information

---

[5] The APPs outline how most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called 'APP entities') must handle, use and manage personal information.

[6] For example, access does not need to be granted to the extent that it would reveal 'evaluative information generated within the entity in connection with a commercially sensitive decision-making process'. See APP 12.3(j)

[7] Agencies, by contrast, must provide access free of charge. See APP 12.7.

through an authorised agent (or in other words, data transfers to third parties are permitted where this is otherwise lawful and in accordance with the APPs).

Credit information

In addition, some banking data constitutes credit information, a subset of personal information. The exchange of credit information (as part of the Australian credit reporting system) is governed separately under Part IIIA of the Privacy Act, and the industry-developed *Privacy (Credit Reporting) Code 2014* (CR Code), approved by me under the Privacy Act.

Part IIIA applies specifically to credit providers (such as banks and other financial institutions) and credit reporting bodies. The provisions in Part IIIA cover various aspects of the handling and exchange of credit information, including the circumstances in which credit providers or credit reporting bodies can collect or share banking data about individuals. Further, Part IIIA and the CR Code set out clear standards in relation to the ability of individuals to access their credit reporting data, including the provision of a free credit report (at least once per year).

As you will be aware, in 2014 significant amendments to Part IIIA came into effect, allowing for a more comprehensive credit reporting scheme. I note that earlier this year the Australian Government indicated an intention to legislate a mandatory comprehensive credit reporting regime, if credit providers are not reporting at least 40% of their data by the end of 2017.

Recommendation 1: the Open banking regime should leverage off the existing regulatory framework

For the reasons outlined below, I believe that the Open Banking regime should be implemented by building on the existing regulatory framework for the handling of personal information.

The Privacy Act is an established, trusted framework that centres on the rights of individuals and the protection of information

The Australian community is increasingly more privacy-vigilant, particularly when it comes to financial data. As part of my Office's *Australian Community Attitudes to Privacy Survey 2017* (2017 ACAPS),[8] individuals were asked what type of information they would be most reluctant to share with an organisation. 'Financial information' was the top response, with 42% of individuals naming this type of data.[9] Related to this, Australians have significant concerns about the use of their data in the online context, due to the potential for identify fraud and other criminal activity. More specifically, the 2017 ACAPS revealed that Australians believe the biggest privacy risks facing the community include:

- online services, including social media sites (mentioned by 32%)
- ID fraud and theft (19%)

[8] Report available on the OAIC's webpage (ACAPS Report).

[9] ACAPS Report, Ibid, p i.

- data security breaches (17%), and
- risks to financial data (12%).[10]

More generally, 58% of Australians have decided to avoid dealing with a private company because of privacy concerns.[11] Further, EY Sweeney's recent *Digital Australia: State of the Nation* (2017) report suggested 68% of Australians worry about what personal information organisations can access about them.[12]

The Privacy Act is a well-established, comprehensive framework which has ensured independent oversight of the regulation of personal information for almost 30 years. Amongst other things, the Privacy Act requires organisations to take reasonable steps to ensure they keep data secure and protected from misuse, interference, or loss; and unauthorised access, modification or disclosure. As outlined above, the OAIC has produced a comprehensive suite of guidance to support organisations to handle personal information appropriately.

Placing the new Open Banking regime within the Privacy Act framework would therefore allow trust to be built, and reassure the community that their sensitive financial details will be handled appropriately, safely, and for their benefit. By contrast, there is a risk that situating any new regime outside the Privacy Act could send a signal that Open Banking represents a shift away from an established, individual-centric, rights-based approach to the handling of personal information, and a tilting in favour of the interests of business.

The Privacy Act successfully balances data protection and competition objectives

The existing Privacy Act framework has a number of different objectives, including:

- to provide the basis for nationally consistent regulation of privacy and the handling of personal information
- to facilitate the free flow of information across national borders (and in the Australian economy), and
- to facilitate an efficient credit reporting system (while ensuring that the privacy of individuals is respected).[13]

In line with these objectives, the Privacy Act has seamlessly integrated competition and data protection objectives in a range of areas. For example, the OAIC's oversight of the consumer credit reporting regime (situated within Part IIIA of the Privacy Act) has ensured public trust in the scheme, and also allowed for a coherent and unified approach to all aspects of the regulation of personal information-handling in both the public and private sectors.

---

[10] See ACAPS Report, above n 4, p i.

[11] Ibid.

[12] Report available at: https://digitalaustralia.ey.com/. See p 93.

[13] See s 3 of the Privacy Act.

A Privacy Code could be used to implement a new Open Banking regime, without the need for complex legislative reform

The ability to access and transfer personal information is already provided for under the Privacy Act in the APPs. The Open Banking regime would therefore represent an enhancement of the existing regime, by articulating more specifically how some of these existing rights should be applied, in a way that benefits individuals.

I note that this specificity could be achieved simply and effectively through the development of a privacy code. A privacy code, developed under Part IIIB of the Privacy Act, would not require legislative intervention to achieve Open Banking objectives. A code could prescribe how APP 12 is to be applied in the banking sector, and could be developed by a nominated code developer, such as an industry body, or an Australian Government agency.[14] Minor legislative amendments to the Privacy Act could still be pursued, if necessary, to support specific policy objectives of the Review – for example, to allow small businesses to access their banking data.[15]

In either case, the development of a code under Part IIIB could allow industry to participate in determining the scope of the new Open Banking scheme, including the type of banking data to be included in the scheme, and the prescribed processes surrounding data access, transfer and security. While industry members themselves would arguably be best placed to develop these data-specifications, if necessary other regulators with relevant expertise, such as the Australian Competition and Consumer Commission (ACCC), could assist with this process.

There are a number of precedents for this option. For example, the Australian Retail Credit Association (ARCA) developed the CR Code under the Privacy Act, which was ultimately approved by me in my capacity as the Australian Privacy Commissioner. Further to this, ARCA developed the Principles of Reciprocity and Data Exchange (PRDE) to enable fuller implementation of the CR Code (and greater participation in comprehensive credit reporting), which was reviewed and approved by the ACCC in 2015. Any breach of the CR Code (as for any Code developed under the Privacy Act) constitutes a breach of the Privacy Act and is therefore enforceable, using the broad range of regulatory powers available to the Australian Information Commissioner under Part V of the Privacy Act.

Building on the existing framework would be efficient and avoid duplication and confusion

A single regulator model for all types of personal information would minimise regulatory burden for industry, by avoiding any potential overlapping of regulatory schemes. In this regard, my Office's regulatory framework in relation to data access and management has already been in operation for over 15 years in the private sector, and has generally been well-integrated by business.

---

[14] See sections 26E and 26G of the Privacy Act.

[15] At present, only natural persons can access their information under APP 12. However, small businesses or other entities could be brought in by way of a minor legislative amendment.

In addition, keeping a single regulator would also avoid confusion for consumers who might otherwise have a choice of regulators to approach with their complaints. It would also ensure that one single regulator can handle all aspects of the same complaint, as complaints about Open Banking arrangements will likely entail other privacy (or personal information handling) issues - for example, disputes about the accuracy of any information transferred.

Given my Office's existing expertise in handling individual complaints about access to personal information held by both the private and public sectors, the OAIC could administer aspects of the Open Banking regime within existing regulatory frameworks, building on existing internal systems and processes. This would result in an efficient scheme, with consistency across sectors and ease of use for individuals. Building on the existing Privacy Act framework would therefore represent a cost-efficient, logical way to implement a new Open Banking regime.

Ensuring consistency with international best practice

Internationally, access to banking or consumer data is primarily viewed as a privacy (or 'data protection') issue, in part due to the influence of the EU's new *General Data Protection Regulation* (GDPR) which will commence, with extra-territorial effect, in 2018. From that time, Australian businesses (including banks and financial institutions) will need to comply with the GDPR if they want to provide goods or services to EU citizens.

Keeping data access and transfer arrangements within the privacy regulatory framework will therefore enable Australian financial institutions to comply with EU privacy law more seamlessly. It will also ensure Australia is able to fully participate in an increasingly internationalised data-exchange market, and avoid the need to develop complex and costly mechanisms to ensure compliance with EU privacy law.[16]

Recommendation 2: Conduct a privacy impact assessment for any proposed Open Banking models

Where a policy or program may have an impact on the privacy of individuals, I recommend that a privacy impact assessment (PIA) be conducted at the earliest opportunity, and preferably in the policy design stage.[17] A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. This process will help to identify any impacts on the privacy of individuals, and allow for privacy safeguards to be built into the preferred regulatory model.

---

[16] For example, the EU-US 'Privacy Shield' framework was developed by the US Department of Commerce and the European Commission (and Swiss Administration), to enable transfers of personal data between the US and the EU to continue, in support of transatlantic commerce. Without such a framework, the legal arrangements in the US for the protection of personal data would be considered 'inadequate' for the purposes of EU data protection law.

[17] I note that my Office has recently developed (and released for public consultation) a draft Privacy Code, which would apply to all agencies covered by the Privacy Act. This Code is likely to come into force in July 2018. One requirement of the Draft Code is that PIAs *must* be conducted for all high privacy risk projects. See the OAIC's website for more information on the draft Privacy Code.

In particular, proposals that involve the creation of standards or systems to facilitate the transfer of data to third parties on a large, automated scale - and particularly financial data, which is considered very sensitive - are likely to raise increased community concern.

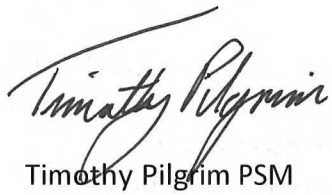
Conducting a PIA at an early stage is the best way to ensure that appropriate privacy safeguards are included in new policy proposals. For more information on conducting a PIA, see the OAIC's *Guide to undertaking privacy impact assessments*.

Next steps

I would be pleased to meet with you and/or your staff in the near future to discuss these matters further, and to offer any other assistance that may be useful to the work of the Review moving forward.

The OAIC contact for this matter is Sarah Ghali, Director, Regulation & Strategy Branch. Ms Ghali can be contacted on (02) 9284 9738 or at Sarah.Ghai@oaic.gov.au.

Yours sincerely



Timothy Pilgrim PSM
Australian Information Commissioner
Australian Privacy Commissioner

15 September 2017