AUSTRALIAN BANKERS' ASSOCIATION INC.
Strong banks – strong Australia

Level 3, 56 Pitt Street
Sydney NSW 2000
Australia
+61 2 8298 0417
@austbankers
bankers.asn.au

29 July 2016

Data Availability and Use
Productivity Commission
GPO Box 1428
Canberra ACT 2601

Dear Sir/Madam

# Issues Paper: Data Availability and Use

The Australian Bankers' Association (**ABA**) welcomes the opportunity to provide comments to the Productivity Commission's (**PC**) Issues Paper *Data Availability and Use* (**Issues Paper**).

With the active participation of its members, the ABA provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services. The ABA works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.

The Issues Paper outlines that a significant public benefit could arise if data collected and stored by government, public bodies and private sector institutions were made more accessible to individuals, third parties and to the general public.

The ABA agrees that increasing access to data could enhance consumer outcomes by facilitating better-informed decision making and more targeted and tailored product and service offerings, as well as allowing customers greater autonomy with their products and services and promoting innovation and efficiencies in the financial system.[1]

Issues for consideration when assessing the need for a policy response to encourage data sharing include:

- If a market failure exists in data sharing
- Maintaining incentives for data investment
- Banks' existing data reporting and costs
- International approaches to data sharing
- Australia's credit reporting system
- Issues of security and privacy of data
- Ownership of data; and
- Access to high value government datasets.

[1] Australian Bankers' Association (March 2015), *Response to Final Report of Financial Systems Inquiry*, p18. http://www.treasury.gov.au/~/media/Treasury/Consultations%20and%20Reviews/Consultations/2014/Financial%20System%20Inquiry%20Final%20Report/Submissions/PDF/Australian_Bankers_Association.ashx

## Is there a market failure?

The ABA notes that the Federal Government's approach to policy making is to ensure that regulation is never adopted as the default solution, but rather is introduced as a means of last resort.[2] The *Australian Government Guide to Regulation* outlines the principles that should be considered when there is perceived market failure.

Using these principles, the ABA believes that for the assessment of data availability and use, this inquiry should consider:

- The state of the market
- The adequacy of the policy and legal framework, setting out the rights of consumers and investors in data and information; and
- An appropriate balancing of private rights and the wider public interest.

The PC's analysis of the expected demand and benefits of data sharing, along with the costs, including security and privacy concerns, will establish if the market-based evolution of data sharing requires policy intervention. The ABA notes that this inquiry arose in part from the Financial System Inquiry recommendation asking the PC to provide evidence of "the costs and benefits to the financial system and broader economy of mechanisms to increase … access to private sector data."[3]

Markets for the exchange of private data have evolved as the commercial benefits have become clearer for both the holders and providers of the data and for the recipient parties, and consistent with community acceptance of such exchange and use of data. This evolution has occurred without specific government intervention or mandate.

The ABA believes the evolution underway in data sharing suggests that government intervention to mandate the release of private data, or to interfere in commercial transactions that underpin the emergence of market solutions, may be unnecessary.

## Incentives for investors in data

This inquiry raises important issues concerning the interests of investors in data, including banks and other commercial enterprises. The banking industry notes that business and customer relationship data are a valuable commercial asset and are subject to extensive investment, privacy and other obligations. Changes should not be made that may affect the ability of businesses to manage their data in the interests of customers and owners.

If data has value and can be sold, then economic incentives exist for the holders of the data to develop the necessary technical solutions and systems to collect, store and protect data. The market will likely provide such systems when commercial incentives and protocols exist. Solutions will emerge as technological, legal and governance issues are resolved.

The ABA emphasises that for this to occur, technology developers need to know they will be rewarded for investments in data. The ABA agrees with the Issues Paper on the need for private returns to justify investments in data, and that tension exists between maintaining commercial incentives while facilitating the release of data which improves efficiency.

Banks are key innovators. Existing financial institutions, including banks, remain largely responsible for successful innovation in financial services in Australia. Mobile banking and new payment technologies are recent examples of financial innovations embraced by customers that were developed and/or rapidly adopted by established players. The evolution of financial technology solutions and better products and services for consumers are primarily the result of private sector initiative and development rather than government regulation.

---

2 Australian Government (March 2014); *The Australian Government Guide to Regulation: Ten principles for Australian Government policy makers,* p2. https://cuttingredtape.gov.au/handbook/australian-government-guide-regulation

3 Financial System Inquiry Panel, November 2014, *Financial System Inquiry Final Report,* http://fsi.gov.au/files/2014/12/FSI_Final_Report_Consolidated20141210.pdf

Strong banks – strong Australia

## Banks in Australia and data reporting

Banks provide significant amounts of data to regulators, customers and third parties.

Banks are required to report a range of data on their products, pricing and operations to regulators such as APRA, RBA, ASIC and AUSTRAC, and to the ABS. These reporting requirements reflect banks' status as Authorised Deposit-taking Institutions and are additional to disclosures required by public companies. Government agencies release significant amounts of this data publicly on their websites and they also provide additional tailored data to academic researchers.

Banks work with customers and other parties in the provision of data. They also report credit history details to credit assessment agencies (more on this below). Banks also report a limited range of data on income earned by customers to the Australian Taxation Office. The information on products used and transaction history is available and readily accessible to customers, and can be passed by these customers to their financial advisers, accountants and other financial institutions. Banks assist this process through, for example, facilitating the input of data into small business accounting systems.

Consideration of the release of additional data on individual customers raises substantive issues that would need to be resolved, including, but not limited to, the ownership of the data, privacy concerns, security, including cyber security, and fraud, including the possibility of identity theft.

## Bank costs of providing access to private data

Other submissions to this inquiry focus on the cost of data dissemination once it is collected, noting that the advent of Application Program Interfaces (**API**) have reduced this cost "towards zero".[4]

The ABA would highlight the significant cost borne by banks in identifying, collating, verifying, aggregating and reporting data, including building and maintaining IT infrastructure, as well as significant ongoing system and compliance costs.

Banks in Australia have invested substantial amounts of time, expertise and money in developing and maintaining systems to comply with all necessary data requirements under Australian laws. In many cases these systems are required to be tailored specifically to a regulator's specifications and to satisfy requirements under specific banking laws.

In 2014, the ABA provided evidence to the FSI panel demonstrating the cost of regulation to banks. The ABA collected data from seven Australia-listed banks[5] relating to the implementation costs (Popex)[6] and ongoing operational costs (Opex)[7] associated with eight streams of regulatory change. The banks were selected to ensure a representation of the costs of large and small banks. On implementation costs alone, the regulations had cost the seven banks $1.73 billion for the eight selected projects. IT costs were the major driver of implementation, but staffing costs were then the major driver of ongoing compliance costs.

Under an Open Banking Standard (**OBS**) (more on this below), a bank would be required to develop and build an API for the purpose of sharing information held about its customer and authorised to be disclosed by the customer. Potentially, the development of an API would entail a bank bringing together or connecting all of its systems, many of which may be compartmentalised and purpose specific involving a variety of data standards and definitions. This is likely to be a very costly exercise for banks based on the experience of implementing other regulatory streams cited earlier. We do not believe that overseas comparisons of costs are appropriate for an Australian initiative.

Any initiative in this space should be based on a rigorous assessment of the likely costs to banks, the take-up by other parties of the data sharing facility, and the benefits that would accrue to consumers.

4 Centre for International Finance and Regulation, July 2016, *Submission to the Productivity Commission on Data Availability and Use*, p6
5 Australia and New Zealand Banking Group Limited, Bank of Queensland, Bendigo and Adelaide, Commonwealth Bank of Australia, National Australia Bank, Suncorp, and Westpac
6 Popex includes implementation costs for a particular project, both those expended, and those budgeted for in the future
7 Opex includes the costs of the first years' operation of the regulatory change

An additional cost of mandating data sharing arrangements would be incurred in protecting the privacy and security of customers' data, both within the bank and in the hands of third parties.

Although it is difficult to establish an accurate figure for the cost of cybercrime in Australia, an October 2013 industry estimate put the cost over the previous year at $1 billion.[8] This is likely to underestimate the total cost of cybercrime as it only includes the cost to individuals affected and omits the cost to business and government.

## International approaches to data sharing

The Issues Paper cites the United Kingdom's OBS as one approach for providing opportunities for third parties to be able to access the personal data of customers.

The ABA wishes to emphasise that the UK proponents of this approach have identified significant technical considerations in defining and implementing an OBS[9]. As observed earlier there would be enormous establishment and operational costs on the banking industry in building the necessary systems to allow internal systems to integrate with a common open standard.

The UK proponents of this approach have also noted critical issues around governance, security, liability, standards, communications, regulation and legal which would need to be resolved. This would equally be the case in Australia.

An OBS is not so much a 'lock key' solution, but rather is a list of issues to be resolved. The ABA suggests that these issues are highly complex and not yet fully expounded or understood. This suggests caution is appropriate.

The ABA is concerned that the benefit of such open systems is explained largely as being to "open business opportunities for third party intermediaries".[10] This infers that the costs of systems and resolving other issues are to be borne by the providers of the data and the primary benefits are to be reaped by third parties. This is not a commercially sustainable policy setting.

The benefits claimed for the use of data by third parties using the OBS may be exaggerated. For example, the UK Financial Conduct Authority (**FCA**) reported in mid-2014[11] that some price comparison websites in the general insurance area did not always ensure that consumers were given the appropriate information to make informed decisions, and were not meeting FCA requirements in delivering fair and consistent outcomes for consumers.

International consensus has not been reached on the most appropriate means of fostering financial innovation. The US Office of the Comptroller of the Currency[12] released a discussion paper in March 2016 on its vision for responsible innovation in the US banking system and the framework for evaluating new and innovative financial products and services. It observed that banks and nonbank innovators can benefit from strategic and prudent collaboration, but did not include any measures for the mandatory sharing of data or open banking standards.

## Australia's credit reporting system

The Issues Paper refers to Australia's consumer credit reporting (**CCR**) regime, noting that this scheme is voluntary, with information to be shared on a reciprocal basis, and is intended to "enhance the decision-making capabilities of businesses in the industry".

The ABA observes that Australia's credit reporting system is the result of a well-established structure of privacy legislation and regulation coupled with industry standards.

---

8 Symantec, (13 October 2013), *2013 Norton Report: Total Cost of Cybercrime in Australia amounts to A$1.06 billion*, Australian Cyber Security Centre, (July 2015), *2015 Threat Report*

9 Open Data Institute (UK), (2015-16), *The Open Banking Standard*, Unlocking the potential of open banking to improve competition, efficiency and stimulate innovation, p3

10 Productivity Commission, Issues Paper: *Data Availability and Use*; p20

11 Financial Conduct Authority, (16 July 2014), *Price comparison websites failing to meet FCA expectations*

12 Supporting Responsible Innovation in the Federal banking System: An OCC Perspective, Office of the Comptroller of the Currency, March 2016

The legislative framework is provided by the *Privacy Act 1988* and the *Privacy Regulation 2013* and the *Privacy (Credit Reporting) Code 2014*.

The operational rules which determine how data is provided and shared are set by the industry. There are a number of elements. The Principles of Reciprocity and Data Exchange is the set of industry-developed data exchange rules which facilitates sharing of credit reporting information. Operational matters regarding the exchange of information between credit providers and credit reporting bodies and the risk assessment process are laid down in the Credit Reporting Code of Conduct. This is a mandatory code that binds credit providers and credit reporting bodies, and supplements the provisions in the Privacy Act and the Privacy Regulations. The requirements for reporting credit accounts between credit providers and credit reporting bodies are governed by the Australian Credit Reporting Data Standard.

The key attributes of these arrangements are that data exchange is voluntary and reciprocal. The ABA generally supports preserving the voluntary and reciprocal nature of the scheme to ensure that benefits are mutually shared, although there is some variation of views among members. A voluntary and reciprocal regime allows credit providers to choose what data they share and with whom they share it. The banking industry continues to work towards greater sharing of data under the current voluntary regime and continues to develop the necessary systems and interfaces.

The ABA generally does not believe that a compulsory scheme would be in the best interests of the industry or of consumers. The ABA supports the relevant part of the Australian Retail Credit Association's submission to this inquiry with effect that CCR should not be mandated.

Whether the use of CCR becomes a necessary element of a credit provider's compliance with responsible lending obligations is a different matter from the Government deciding to mandate the CCR regime itself.

The ABA submits it would be premature for the Government to mandate CCR for a number of reasons.

First, there has been a significant amount of investment by industry in CCR. This investment should be allowed to come to fruition before regulatory mandates are considered.

Second, the Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* states that it was not an objective of this Act to regulate all aspects of CCR. Industry was free to choose some credit reporting issues such as reciprocal sharing of information between industry participants in the credit reporting system[13] which industry has done and is continuing to do.

Third, mandating CCR will not deal with key issues affecting the rollout of CCR. An example of a key current issue concerns how consumer credit customers who experience financial difficulties in meeting their commitments are to be reported under CCR, particularly in respect of repayment history information (RHI).

The issue is whether customers who are accommodated under their banks' financial hardship arrangements may be identified under RHI. The industry proposes that a hardship flag be included with RHI to help explain any missed payments. This would signal to other credit providers to be wary in advancing further credit. In the absence of an explicit warning such as this, other credit providers may assume that the customer is meeting his or her obligations when in fact their credit provider is refraining from collection activity to allow the customer time to recover their financial position.

The alternative view that the inclusion of a hardship flag would deter customers in financial hardship from approaching their credit provider(s) for assistance is difficult to sustain. Banks continue to be on the front foot in making the availability of their financial hardship relief programs known to the community and these programs are understandably well utilised by those customers who need some form of relief.

The ABA welcomes the Government supporting current industry efforts to expand data sharing under the new CCR regime and to facilitate resolution of key issues.

[13] https://www.legislation.gov.au/Details/C2012B00077/Explanatory%20Memorandum/Text

The ABA in its submission to the Government's response to the Final Report of the Murray Financial System Inquiry supported the Government's backing for current industry efforts to expand data sharing under the new CCR regime rather than through legislation.

## Ownership of data

The question of the ownership of data is posed in the Issues Paper as:

> *Who should have the ownership rights to data that is generated by individuals but collected by businesses? For which data does unclear ownership inhibit its availability and use?*

Creating a right of property in information itself would be inconsistent with the way the law in Australia has developed. The High Court of Australian in *Breen v Williams*[14] established that there is no general right of property in information.

To assign a proprietary right in information to a particular class of entity or individual would result in the general rules of property law applying to that right. This would, for example, include the attributes that property is by nature divisible, transferable and able to be held as security for the performance of contractual obligations.

The Privacy Act is not a proprietary regime concerning an individual's personal information. The Act confers on the individual protective rights with respect to their personal information. These rights are not indicators of ownership but rather a source of a human right.

The UK OBS is not dependent on the question of who owns what data. It is an access model based on authorisation and confidentiality and privacy considerations.

The predominant category of data generated by a bank customer is the customer's application and transactional data. This information is collected by the bank in order to comply with a wide range of legislative requirements such as the National Consumer Credit Protection Act, the Corporations Act (Ch7), AML/CTF legislation, taxation legislation and for the purposes of reporting to key banking regulators i.e. APRA and ASIC.

These datasets are also necessary for the bank to provide an appropriate level of service to the customer. To do so, banks have invested very substantial amounts of time, expertise and money to design, build and operate and maintain the necessary data systems. The unique ability of the bank to harness, classify, record, report and retain systematically the customer's personal information which the customer would be unable, or be prepared, to do, points to the question of ownership in favour of the bank.

For banks, the question of the proprietorship of customer data does not arise in the ordinary course of bank and customer relationships. In terms of the Commission's question about unclear ownership of data and whether this could inhibit its availability and use, the ABA's view is that introducing proprietorship concepts for data collected by banks about their customers would lead inevitably to complication and uncertainty. This could, of itself, create barriers to the availability and use of data.

The market for dissemination of an individual's personal information does not appear to be inhibited by questions of ownership (unless protected by intellectual property law, for example, by copyright) other than, in the main, by the Privacy Act.

Individual customers have rights of access to, and correction of, the personal information held by banks about them. With many customers using internet banking facilities, their transactional data is readily available at any hour or day.

The ABA considers that the private sector should retain its incentive to continue to invest in, innovate, develop and enhance its data collection and management of information. One measure to assist this is to provide an excludable right in favour of makers of databases to protect these data from unauthorised use. The right would not be proprietary in nature.

[14] (1996) 186 CLR 71 also at http://www.austlii.edu.au/au/cases/cth/HCA/1996/57.html

The Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases[15] provides an example of this excludable right. Article 7 of the Directive makes provision for a right for a maker of a database which shows there has been a substantial investment in obtaining, verification or presentation of the database contents to prevent unauthorised extraction or publication of all or a substantial part of the database.

## Privacy concerns

The community in general is increasingly sensitive to privacy concerns, despite the protections in the Privacy Act, as well as cyber security. In the Office of the Australian Information Commissioner, *Community Attitudes to Privacy survey*, Research Report 2013[16] it is reported that:

> *"Australians believe the biggest privacy risks facing people are online services - including social media sites. Almost a half of the population (48%) mentioned these risks spontaneously. A quarter (23%) felt that the risk of ID fraud and theft was the biggest, followed by data security (16%) and the risks to financial data in general (11%)."*

Any move to mandate sharing of large amounts of data would raise significant issues for banks and their customers, and obligations on third parties.

## High value government data sets

The Government and regulators can encourage innovation through the introduction of trusted digital identities. Developing a national strategy for a federated-style model of trusted digital identities was a key recommendation made in the final report from the Financial System Inquiry. The banking industry supports this recommendation as a means of complementing financial system innovation, lowering costs and lowering risks for the industry, customers and other stakeholders. The ABA would encourage the PC to examine how the Government can hasten the development of digital identities.

Digital identity relates to how parties, be they individuals, businesses or government, can confirm the identities of other parties for online financial transactions. It relies upon identity verification using attributes such as name, date of birth and address using government-issued, paper-based credentials like drivers' licences and passports. Based on this the individual receives an identity authentication such as login and password, and potentially more sophisticated measures such as e-certificate or potentially biometric data.

There are shortcomings in accessing government-held identity data. For example, banks are currently able to access the electoral roll to verify a customer's details when they apply to become a customer, but are unable to use the electoral roll to update their details once they are a customer. Voters updated their details with the Australian Electoral Commission prior to the recent election, but banks were unable to utilise this updated information to verify their customer contact details.

The ABA looks forward to further engagement with the PC on the issues raised here and by others through the consultation process.

Yours faithfully

Signed by

Tony Pearson
Chief Economist & Executive Director, Industry Policy
tony.pearson@bankers.asn.aus

[15] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML
[16] https://www.oaic.gov.au/engage-with-us/community-attitudes/oaic-community-attitudes-to-privacy-survey-research-report-2013#4-detailed-findings