NATIONAL AUSTRALIA BANK SUBMISSION

Productivity Commission Draft Report: Data Availability and Use

12 December 2016

Overview

National Australia Bank (NAB) welcomes the opportunity to provide feedback in response to the Productivity Commission's (PC) 'Data Availability and Use' inquiry draft report. As a member of the Australian Bankers' Association (ABA), NAB has also contributed to and is supportive of its submission.

NAB welcomes competition and, as previously stated publically, supports data sharing in principle if it can generate better outcomes for customers.[1] The security and safety of NAB's customer data is paramount, so sharing of data should be done with correct protocols and security regimes in place. Moving to an open data regime without appropriate safeguards and requirements could raise significant security concerns. If data or privacy breaches occurred during the sharing of customer data – either caused by NAB or a third party– this could significantly impact on the trust and confidence that customers have when dealing with NAB.

NAB has focused its response on certain sections and draft recommendations of the report which it believes will be most useful to the PC. These are comprehensive credit reporting (CCR) (Chapter 4 – Private sector data collection and access); the sharing of data via open application programming interfaces (APIs) (Chapter 6 – Make data useful); and, the proposed comprehensive right (Chapter 9 – A framework for Australia's data future).

NAB supports the benefits that CCR will offer consumers and believes these are best delivered via a voluntary system with the active participation of industry.

On open data, NAB is pursuing several streams of work related to APIs but urges caution against the mandatory sharing of data due to the impact on existing industry work and innovation, the likely cost incurred and the importance of ensuring appropriate security.

In relation to the proposed comprehensive right, NAB believes that mechanisms proposed under the right are already available through existing Australian Privacy Principles (APP) and other provisions of the *Privacy Act 1988 (Cth)* and directs the PC to this legislation.

[1] See: Antony Cahill, NAB Chief Operating Officer, House of Representatives Standing Committee on Economics, Hansard, Thursday 6 October, p7.

1. Comprehensive Credit Reporting (CCR)

Draft recommendation 4.1 (p170)
The Australian Government should adopt a minimum target for voluntary participation in Comprehensive Credit Reporting (CCR) of 40% of accounts. If this target is not achieved by 30 June 2017, the Government should circulate draft legislation to impose mandatory reporting by 31 December 2017.

1.1 NAB participation in CCR

NAB has led the major banks in the implementation of CCR and has been sharing data in 'private' mode with all three credit reporting bodies since August 2015. NAB remains the only major bank doing so. NAB believes that a CCR environment with participation by all lenders will:

- Support more accurate pricing of credit;
- Improve access to credit for consumers who may traditionally have found it difficult to access credit from a major lender; and
- Promote greater competition among lenders, which ultimately benefits consumers.

NAB supports voluntary CCR participation while recognising that successful implementation of CCR requires active participation by all credit providers. NAB believes voluntary participation will provide the optimal way for institutions to participate and ensure customers get the best possible benefits from the CCR system.

1.2 Obstacles to sharing CCR data

NAB's CCR development is relatively well progressed, with an intention to have all necessary infrastructure and supporting processes in place to enable full CCR participation during 2017. As an early adopter, NAB has also invested significantly in confronting broad industry issues experienced during implementation.

The most significant issue encountered to date is a Financial Ombudsman Service (FOS) determination made in April 2016. As the PC notes,[2] the determination about the reporting of repayment history information (RHI) for customers under payment arrangements has created uncertainty about reporting requirements under CCR. This determination has generated a risk to NAB's implementation timeline as differing requirements could impact the internal technology and systems already developed to facilitate full CCR participation.

While CCR was legislatively enabled in early 2014, as the PC notes,[3] the framework required to facilitate CCR participation – the Principles of Reciprocity & Data Exchange (PRDE) – was only completed in December 2015. Given this, having a benchmark assessment date of mid-2017 (as the PC has proposed in draft recommendation 4.1) provides insufficient time to assess whether voluntary participation has been successful. NAB submits that a preferable benchmark date would be 31 December 2017, allowing a full two years post the required framework being approved.

NAB is not in favour of mandatory CCR and believes attention should be focussed on addressing the obstacles preventing NAB and other early adopters from sharing CCR data. While uncertainty persists around reporting of fundamental elements such as RHI and potential changes to elements of the framework, it will be difficult for NAB to move to a shared CCR environment.

1.3 Potential mandatory framework

As noted in Appendix E, mandatory participation would likely require a high level of prescription for reporting data, which may then not keep pace with the changing consumer and industry

[2] Productivity Commission, Data Availability and Use, Draft Report, p169.
[3] *Ibid*, p549.

requirements.[4] Mandatory reporting could also create data quality issues given the significant increase in the amount of data required to be reported.[5] NAB shares these concerns.

As an early adopter, any changes to the current voluntary requirements would impact NAB more than others, and NAB would in effect be penalised for choosing to be an early adopter. If a mandatory approach was pursued at some point in the future, NAB would recommend mandating utilisation of the existing framework the industry has developed, rather than redefining this framework. An alternate approach would likely require costly re-work of the investment NAB has already made to date to implement CCR.

NAB's View

- Supports a voluntary system for CCR participation while recognising that successful implementation of CCR requires active participation by all credit providers.
- Believes a benchmark date of 31 December 2017 is best to assess whether voluntary participation has been successful.

2. Open Data

Draft recommendation 6.2 (p248)

The private sector is likely to be best placed to determine sector-specific standards for its data sharing between firms, where required by reforms proposed under the new data framework. In the event that voluntary approaches to determining standards and data quality do not emerge or adequately enable data access and transfer (including where sought by consumers), governments should facilitate this, when deemed to be in the public interest to do so.

Information Request (p250)

The Commission seeks more information on the benefits and costs of a legislative presumption in favour of providing data in an application programming interface (API) format, specifically:

- In which sectors would consumer benefit from being able to access data in an API format?
- What are the main costs and barriers to implementing APIs?

In principle, NAB agrees with sharing customers' data with other institutions,[6] providing the appropriate security arrangements are in place and that institutions which receive this data accord the same high premium to data protection as NAB does. With these safeguards in place, greater sharing of data offers the ability to enhance competition and improve consumer outcomes.

Before addressing the PC's information request and draft recommendation, for the PC's background below is an outline of what NAB has done and is currently pursuing in relation to APIs.

2.1 NAB's use of APIs

NAB and other major banks are proactively pursuing the improved sharing of data and use of open APIs. APIs were first implemented as part of the NAB technology infrastructure in 2013. Since then, APIs have been an important part of NAB's digital infrastructure. NAB's digital assets are currently in the process of being API enabled (e.g. NAB's update to mobile banking applications on Android and IOS in October and November respectively 2016 was underpinned by APIs). This enablement will provide greater flexibility for sharing data.

Over the past three years, NAB has been progressing three streams of API related work:

---

[4] Productivity Commission, Data Availability and Use, Draft Report, p549

[5] *Ibid*, p550.

[6] See: A Cahill, NAB Chief Operating Officer, House of Representatives Standing Committee on Economics, Hansard, Thursday 6 October, p7.

1. **Internal**: NAB's internal technology infrastructure has been transformed to be API enabled.
2. **Partner:** NAB has partnered with key organisations to offer innovative solutions via APIs. Examples include sharing data with accounting software provider Xero (see case study below).
3. **Open:** NAB is currently classifying APIs into categories and identifying those suitable for a trial release, with access to publicly available data through a portal being a likely first step in a trial.

NAB will continue to proactively foster further data sharing through each of these streams of work.

2.2 Case Study: NAB partnership with Xero

Sharing NAB transaction data to Xero
NAB shares banking information relating to small businesses customers with accounting software provider Xero. Xero's all-cloud environment connects with NAB in a partnership announced in April 2015. NAB was the first Australian bank with core API technology linked to Xero's accounting cloud ecosystems. NAB small business customers are able to access this functionality via their internet banking account.

Sharing Xero accounting data to NAB
Xero shares authorised customer accounting data with NAB to help enable lending assessments for NAB's innovative new small business lending product, QuickBiz Loans. The online application provides businesses with a lending decision for unsecured funding of up to $50,000 within 60 seconds with funds available within three business days after approval.

2.3 Determining standards

NAB agrees with draft recommendation 6.2 though that the private sector is *'best placed to determine sector specific standards for its data sharing between firms'* and urges caution against the adoption of statutory mandatory requirements for data sharing.

NAB's four reasons for supporting this draft recommendation are:

1. Potential to impact on innovation already occurring
The imposition of a mandatory standard would stifle the innovation currently occurring within the banking sector (see above three streams of work for NAB) on how APIs can be utilised. This activity, particularly partnering and sharing open APIs in the future, creates competition within the sector to best meet the needs of consumers. A mandatory standard would likely cause some of this work to be redirected towards meeting a mandatory requirement and ensuring data can be shared in the obligated format.

Banks would no longer be incentivised to compete in the provision of customer data, as they currently do in the provision of other digital services such as payments, systems and applications. A mandatory scheme may offer some short-term uplift in the amount and formatting consistency of data, but in the medium to longer-term, consumers may not experience the full benefits of APIs which can be developed through the careful consideration currently taking place at NAB.

NAB also believes that different customer types will have different needs and uses for their data, allowing banks to vary the way this data could be made available. Mandatory sharing of data in prescribed formats would likely limit the ability for NAB to provide data in a more bespoke format for customers meaning that some may not experience the full benefits from the data. In addition, NAB believes that legislating prescriptive technical solutions could become out-dated as technology changes.

2. Cost
The cost of implementing statutory or regulatory mandatory data sharing requirements is likely to be significant. The key costs will be in identifying, collating, verifying and aggregating the data, the development of technology systems and infrastructure to complete this work and the ongoing costs of data reporting and system maintenance. It is difficult to estimate the specific costs

without a proposed approach, data format and commencement date being identified. NAB supports the ABA though in believing that overseas comparisons of costs for implementing open banking standards and APIs are not appropriate or accurate guide for Australian costs.[7] An example of a recent industry investment in another large scale technology solution is the New Payments Platform (NPP).

Investment to date by the industry to innovate in this area is significant, but the costs associated with a mandated regime are likely to be far higher for NAB. NAB also notes that the costs for implementing more open standards are likely to be borne by the banking sector with the initial beneficiaries to be third parties, a situation which is not commercially sustainable in the long-term.

3. Security

The security of any shared data should be paramount. If consumers were able to request their data be provided directly to third parties on request, NAB could be unaware of a third party's data management standards and practices and if they were in keeping with NAB's own high standards and the expectations of customers.

NAB is currently managing the security risks associated with APIs in a careful and considered manner, utilising existing expertise in this area and in line with NAB's existing risk appetite. A mandated scheme and approach would make it harder for NAB to manage this risk on behalf of its customers. Breaches by a third party of NAB-provided customer data could have a greater impact on the customer's relationship with NAB than the third party. Research from the World Economic Forum suggests that financial institutions are typically 'trusted by consumers beyond other institutions to be safe repositories of information and assets'.[8]

4. Uncertainty

NAB understands that certain competitors are seeking access to customer and small business data. NAB does not have a complete view of how Financial Technology (Fin Tech) firms plan to use this data. Gaining greater clarity on what the actual consumer benefit will be from sharing this data is important in determining what type and format of data is most appropriate to share. NAB believes this clarity will evolve over time.

2.4 If mandated data sharing requirements were adopted

While NAB urges caution against the adoption of a mandated data sharing requirement, if such a standard were to be considered then NAB would suggest it be conducted in a test and learn environment. The considerations of this approach should include:

- **Definition of data and data categories:** Define the relevant consumer data as data collected from customers (i.e. raw data), not insights that banks derive from that raw data which NAB considers is proprietary. Limiting the scope of data to non-authenticated and 'read only' authenticated data would assist in best managing security risks.
- **Restrictions on third party use of the data:** Limit the use by third parties so that it cannot be interwoven with data from competitors to enable 'aggregator banks' to be created. These could control the customer interface to their banking but not incur the cost of the underlying maintenance of that data and servicing. If such aggregator models were to exist, this could be enabled through a commercial arrangement with banks as a provision of service.
- **Third party accreditation:** Provide the ability to restrict third parties that can access APIs to those parties which offer appropriate security protection.
- **Liability regime:** Liability for fraud or data misuse caused by the transfer of data to a third party should fall with that entity (see p10).

[7] Australian Bankers' Association, 'Submission to the Productivity Commission's Issues Paper, *Data Availability & Use'*, 29 July 2016.

[8] World Economic Forum 2016, p23, (in conjunction with Deloitte), 'A Blueprint for Digital Identify: The Role of Financial Institutions in Building Digital Identity'.

- **Use limits:** A limit to API calls over certain timeframes to ensure the running of existing banking infrastructure is not compromised.

NAB's View

- NAB is proactively pursuing the improved sharing of data and use of open APIs through three streams of API related work.
- Urge caution against the adoption of statutory mandatory requirements for data sharing due the impact on innovation already occurring, the cost of mandating and ensuring appropriate security concerns.

3. Making data more useful

Draft recommendation 9.1 (p346)

The Australian Government should introduce a definition of consumer data that includes:

- personal information, as defined in the *Privacy Act 1988* (Cth)
- all files posted online by the consumer
- all data derived from consumers' online transactions or Internet-connected activity
- other data associated with transactions or activity that is relevant to the transfer of data to a nominated third party.

Data that is transformed to a significant extent, such that it is demonstrably not able to be re-identified as being related to an individual, should not, for the purposes of defining and implementing any Comprehensive Right, be defined as consumer data.

The definition of 'consumer data' should be provided as part of a new Act regarding data sharing and release (Draft Recommendation 9.11). Given the need for this definition to have broad applicability, it should also be included within the Acts *Interpretation Act 1901* (Cth). Consequential amendments to other Commonwealth legislation would ensure harmonisation across federal laws.

Draft recommendation 9.2 (p350)

Individuals should have a Comprehensive Right to access digitally held data about themselves. This access right would give the individual a right to:

- continuing shared access with the data holder
- access the data provided directly by the individual, collected in the course of other actions (and including administrative datasets), or created by others, for example through re-identification
- request edits or corrections for reasons of accuracy
- be informed about the intention to disclose or sell data about them to third parties
- appeal automated decisions
- direct data holders to copy data in machine-readable form, either to the individual or to a nominated third party.

Individuals should also have the right, at any time, to opt out of a data collection process, subject to a number of exceptions. Exceptions would include data collected or used as:

- a condition of continued delivery of a product or service to the individual
- necessary to satisfy legal obligations or legal claims
- necessary for a specific public interest purpose (including archival)
- part of a National Interest Dataset (as defined in Draft Recommendation 9.4).

The right to cease collection would not give individuals the capacity to prevent use of data collected on the individual up to the point of such cessation.

The existing legislative framework

Rights and obligations under the Privacy Act

Entities are required to provide data to individuals when it is considered *personal information* under s6 of the Privacy Act (where the information relates to an identifiable individual or an individual who is reasonably identifiable). Identifiable information, including digital data, transactional data and credit eligibility information, is subject to the existing privacy framework. This ensures individuals can access, seek correction of and complain about the use or misuse of this information. Individuals must also be notified about the fact of collection, purposes of collection, consequences for the individual if the information is not collected, entities to whom the information is usually disclosed and whether the information is likely to be disclosed to overseas recipients. In addition, organisations must obtain individuals consent to the sharing and transfer of certain information, such as credit information, with third parties (such as credit providers, guarantors and mortgage insurers).

NAB supports mechanisms to provide consumers with access to certain data held about them. NAB believes these mechanisms are currently available through the more effective utilisation of existing legislation.

While the Privacy Act articulates this framework as a series of positive obligations on entities, NAB believes that, in practice, this is utilised by consumers and respected by organisations as comprising a comprehensive set of consumer rights to their information. For these reasons, NAB considers that the proposed 'consumer data' is already covered under the Privacy Act and additional legislation for this type of information is unnecessary and will result in duplication and uncertainty for businesses and consumers.

NAB recognises the PC's aspiration to improve consumer awareness of data as an asset and supports measures to increase knowledge of the value and availability of data held by organisations. To date, formal access requests by NAB customers for data have been primarily connected with a dispute, rather than individuals making an isolated access request. NAB has not experienced customer dissatisfaction with the type, format or amount of information they are being provided. There is also no indication that customers do not understand the information as it is presented.

To address any perceived disparity between the nature and level of information made available to consumers under the existing legislative framework, NAB is open to working with industry and consumers to increase awareness and utilisation of the existing rights of data access and transfer conveyed under the Privacy Act.

As outlined above, the proposed new rights in draft recommendation 9.2 of access, correction, notification of collection and consent to information disclosure or sharing with third parties, currently exist under the Privacy Act in relation to personal information. NAB notes that in relation to the right of access to data 'created by others, for example through re-identification', the Privacy Amendment (Re-Identification Offence) Bill 2016 (Cth) is currently before Parliament and may impact the rights of consumers in the future under the proposed comprehensive right.

Express exceptions to the Comprehensive Right and 'consumer data'
Notwithstanding the above comments, should the PC recommend introducing a definition of 'consumer data' in the final report, NAB proposes that the definition expressly articulate certain exceptions to the definition as it exists in the draft report.

Specifically, the reference to 'all data derived from' can have far-reaching implications as online transactional information and internet-connected activity is used as part of a number of NAB internal classifications (e.g. segmentation, pricing and fraud propensity), process and operations. This type of information can be distinguished from 'raw data' and NAB considers it to be commercially sensitive and proprietary. NAB notes that under APP 12.3(j), entities are not required to give consumers access to data where it would 'reveal evaluative information generated within

the entity in connection with a commercially sensitive decision-making process'. NAB supports the need for a similar exception under any new proposed definition of 'consumer right' to ensure consistency with existing legislation.

NAB believes that exceptions should also be included for data collected and provided to regulators such as AUSTRAC and ASIC, where provision of the data to the consumer could prejudice enforcement related activities (see also APP 12.3(h) and (i)).

Additionally, to the extent that 'other data associated with transactions or activity that is relevant to the transfer of data to a nominated third party' refers to assessments of veracity or interpretation of data, NAB believes that it would be prohibitively costly to require data holders to warrant that the data is complete and accurate. NAB proposes that data holders be required instead to provide a transparent assessment of the veracity of any data provided to a consumer or third party, and that data holders not be liable for any subsequent interpretation of data by consumers or third parties.

Innovation and competition

NAB does not support the view that the proposed definition of consumer data will incentivise deliberate de-identification of data holdings. NAB does not consider that the degree of regulation in the sector creates a weaker incentive to innovate or meet the interests of consumers.[9] As one example, the banking sector is already improving the ability of consumers to access data and working to deliver innovative customer outcomes. The New Payments Platform (NPP) will introduce a new payments model with rich data transfer at its centre. Under NPP, customers will have an account identifier which will enable them to link a unique piece of data (such as their email address, mobile number or ABN) to their preferred bank account; a capability which NAB believes will enhance the ability of customers to switch between banks and promote competition.[10]

The development of NPP is premised on further innovation and collaboration with industry partners. In the future, new NPP Overlay Services (apps) will have the potential to enable payments to go beyond value transfer.[11] The ability for NPP to create customer value will increase exponentially, the greater the participation of financial institutions and new entrants.

Draft recommendation 9.4 (p358)

The Australian Government, in consultation with state and territory governments, should establish a process whereby public and private datasets are able to be nominated and designated as National Interest Datasets (NIDs). Datasets (across the public and private sector) designated as NIDs would satisfy an underlying public interest test and their release would be likely to generate significant community-wide net benefits. Designation would occur via a disallowable instrument on the recommendation of the National Data Custodian. NIDs that contain non-sensitive data should be immediately released. Those NIDs that include data on individuals would be available initially only to trusted users and in a manner that retains the privacy of individuals and/or the confidentiality of individual businesses. The in-principle aim should be for these de-identified datasets to be publicly released in time. The process to designate datasets as being of national interest should be open to the states and territories in order to cover linked datasets, with negotiations undertaken to achieve this. For community confidence, consideration should be given to use of a deliberative forum, such as a parliamentary committee, to take community input on and review nominations made, and to make proposals for future designations.

[9] Productivity Commission, Data Availability and Use, Draft Report, p172.

[10] See: NAB response to Question on Notice 3, House of Representatives Standing Committee on Economics, 20 October 2016.

[11] See: NAB, 'What's the future look like for Real Time Payments?' 10 November 2016, <http://news.nab.com.au/whats-the-future-look-like-for-real-time-payments/>, 10 November 2016.

The report references an 'underlying public interest test' and requests further information on datasets that are of national interest.[12] NAB agrees with the PC's position that NIDs containing identifiable data only be released in de-identified form;[13] any information that is contributed to a NID should be incapable of being re-identified in the hands of the Australian government and/or trusted users. Further, the process of de-identification should occur at the individual contributor level so the information shared is de-identified. Appropriate security controls and frameworks would need to be developed with each of the trusted users to whom the information would be disclosed. NAB notes that the Privacy Act would not apply to NIDs to the extent that they are permanently de-identified datasets.

In addition to the Privacy Act, a bankers' duty of confidentiality and the Code of Banking Practice, which codifies the duty for small business and consumer customers, should be considered.[14] Exceptions to this duty include where disclosure is 'compelled by law' or where there is a 'duty to the public' to disclose. Any requirement to disclose information as part of a NID should be categorised as requiring disclosure under law and linked to a defined public interest purpose. This would help ensure disclosure does not contravene the banker's duty of confidentiality or the Code of Banking Practice.

NAB notes that one of the proposed sources of data for the NIDS is 'all data collected in the course of meeting regulator requirements'.[15] Some information currently disclosed under regulatory requirements may be highly confidential and commercially sensitive to the contributor, for example if it relates to breach notifications, taxation records or financial records. Accordingly, NAB does not believe that all data collected in the course of meeting regulatory requirements should be 'automatically incorporated by requirement' into NIDs.[16]

NAB's View

- Supports improving consumer awareness of existing data rights and obligations.
- Considers the existing framework under the Privacy Act can be utilised to realise the PC's aspirations for consumer's access to their data.
- Believes any final recommendation under 9.1 and 9.2 should include express exceptions consistent with existing legislation.

4. Data security and privacy breaches

NAB supports an economy-wide regulatory scheme which sets out the obligations and liabilities of data holders, consumers and third party users of data to ensure that the rights and responsibilities of each data sharing participant is clearly identified. In particular, the obligation on a data holder for data breaches should be to ensure appropriate contractual provisions are included in any data sharing agreement with respect to data quality, security, retention, destruction, monitoring and reporting and to effectively manage ongoing compliance with these requirements. A data holder should not be liable for actions resulting in data breaches that amount to a breach of contract by the data user or which could not have been detected through contracted monitoring or oversight activities. NAB considers that the existing framework under the Privacy Act and Office of the Australian Information Commissioner is the most appropriate mechanism to provide guidance on these issues.

NAB's View

- Supports the introduction of an economy wide regulatory scheme to address obligations and liability for data security and privacy in connection with data sharing and transfers.

---

[12] Productivity Commission, Data Availability and Use, Draft Report, p354.
[13] *Ibid*
[14] An independent review of the Code of Banking Practice is currently being undertaken by Phil Khoury as part of the six ABA initiatives announced in April 2016. This review is due to be completed by the end of 2016.
[15] Productivity Commission, Data Availability and Use, Draft Report, p356
[16] *Ibid*