Australian Banking Association

30 June 2022

Alison Frame
Deputy Secretary, Social Policy

Dear Ms Frame

Consultation on the Australian Data Strategy

Thank you for the opportunity to comment on the Australian Data Strategy ('the strategy'). The Australian Banking Association (**ABA**) welcomes the development of a unified strategy around the use of public and private data to drive economic, health and social outcomes. We are optimistic that all Australians will benefit from a coordinated government approach.

Maximising the value of data

Australian banks have long shared data with government as well as being subject to government initiatives requiring data sharing with non-government entities. The costs that are borne by banks in participating in these data sharing arrangements are substantial, and do not always appear to have equivalent benefit for customers, while removing resources from other initiatives that could potentially be of more benefit. An assessment of costs relative to benefits should inform whether to proceed with any government-driven data collection initiatives.

Banks encourage Government to use data sources already collected from the private sector to avoid duplication and rework by private sector entities. APRA's development of flexible data collections is expected to be a good source of data which can be drawn upon in times of crises. Finally, banks welcome the opportunity to access customer data held by government to support more timely and accurate decision-making.

Trust and protection

Data security and privacy remain two of the areas which banks support strong legislative protections for the benefit of their customers. We encourage Government to work with industry to develop a principles-based approach to any future governance, including for AI. We acknowledge the need for clear consumer consent when sharing consumer data and welcome a standardised approach to data retention practices.

Enabling data use

For ease and efficiency, we encourage legislative simplification, including identification of any legislative tension which can lead to outcomes that are odds with the intended goal of government-driven data initiatives. We also encourage Government to invest in appropriate skill development to support a strong data economy within Australia. Industry benefits from access to a skilled pool of labour from which to draw. This labour may be accessed via skilled migration or developed through vocational and tertiary training.

Finally, we recommend that future strategies draw on the lessons learned from the development of similar strategies in other jurisdictions.

Yours sincerely

Michelle Jakubauskas

About the ABA

The Australian Banking Association advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

Australian Banking Association

Maximising the value of data

The Australian banking industry has a long history of sharing data with the Australian Government to support public initiatives. Banks are currently subject to a number of regulatory regimes that require the sharing of institutional and customer data to government agencies or to other data recipients.

For example, banks share data with government as part of anti-money laundering / counter terrorism financing (**AML/CTF**), tax, prudential and corporate supervision, as well as other ad hoc regulatory projects by members of the Council of Financial Regulators. Banks also share data as a result of government-driven initiatives including the Consumer Data Right (**CDR**), which requires banks share data with accredited data recipients and Comprehensive Credit Reporting (**CCR**) which requires the sharing of customer data with other lenders.

Banks also provide substantial data to government by way of Economic and Financial Statistics. This is information generated as part of the day-to-day activities in the banking industry, which is essential to much of the macroeconomic policy development undertaken by government agencies such as Treasury and the Reserve Bank of Australia (**RBA**) as well as private entities and academic researchers.

Further to this, banks are asked to deliver data to government above and beyond ongoing regulatory requirements, including providing data to support public responses in times of emergencies. For example, during COVID-19 ABA members provided substantial amounts of data to Treasury, the Australian Bureau of Statistics (**ABS**) and the Australian Prudential Regulation Authority (**APRA**). This data provided insight into the financial experience of Australians and the economy which guided many of the emergency fiscal policy measures implemented by Treasury in response to the crisis.

Holistic approach to government accessing data held by banks

Given this, banks are at the forefront of implementing data reporting systems, having made significant investments to ensure the benefits of data sharing are maximised while also maintaining the safety and security of customer data. While there is some headway being made towards greater coordination of government agencies when it comes to collecting data from industry, this could be even further improved.

ABA members support a whole-of-government approach to data collection which avoids duplication and the use of unnecessary resources by industry. Banks anticipate investing substantial resources into developing the infrastructure to meet APRA's new data collections and consider this one of the largest government data projects in operation. However, there is no mention of this initiative in the strategy.

Regulatory reporting via APRA involves substantial consultation on the collections which are compiled on regular monthly, quarterly and annual bases. Banks apply rigorous auditing and governance processes to these collections, providing a level of trust in the data which leaves banks.

Separately, banks receive ad hoc requests from government departments which do not go through central regulatory reporting mechanisms. This can result in duplication of data being shared with government agencies and raises questions of the extent to which government agencies are communicating with each other about data that is already collected.

While we do not encourage free sharing of bank data between government agencies, we do request consideration of data which is already held by government when requesting data from banks. For example, sharing of private sector data between government agencies and third parties, as outlined in the Data Availability and Transparency Bill ('**DAT Bill**'), does not provide adequate assurance the bank data will not be misinterpreted, used to identify commercially sensitive information, or have appropriate governance applied to it.

Equally, different government agencies requesting private sector data in a series of uncoordinated data requests can result in duplication, data quality issues and associated resubmissions to overcome data quality issues. Therefore, there needs to be a way for government to have a coordinated approach to accessing and using private sector data, with assurance that end users apply appropriate protections and do not misuse the data.

Costs and benefits of sharing private sector data

The strategy makes clear that 'the cost of inaction is high'. However, the experience of banks shows that the cost of action is not always met with the equivalent benefits to Australians. As the Australian Government looks to unlock more private sector data, it is important that all data sharing arrangements are underpinned by feasible use cases which show value to the Australian community. Where there is no clear evidence of this, industry should not be required to place substantial investments in data architecture & associated systems.

Depending on how it is to be done, sharing data can require large investments in data infrastructure to ensure that the data is transferable, aggregable, and otherwise usable. Every corporate entity has unique metadata and ways of storing data. Bringing these disparate datasets together requires changes to data architecture to standardise the data and thereby make it comparable and collatable. The wider the scope of data sharing, the larger the investment required of firms.

For example, ABA members have invested over $1 billion to meet the regulatory requirements to establish data sharing under the CDR and continue to invest in developing capabilities towards becoming Accredited Data Recipients (**ADRs**) or forming use cases that benefit consumers. There are substantial costs associated with projects coming from the detailed specification of metadata.

At this stage, there are several datasets that banks have built that have little or no benefit to consumers that do not use the products involved in the build, or larger institutional clients that have alternative ways of receiving data on their activities. We support a better evaluative process to understand the benefits that data sharing would have for consumers and the wider economy and to prioritise data sharing where the value to consumers and the economy are clear and appropriate to the cost on business and the government in providing those services. Money that is invested in data schemes that yield little benefit for consumers could be better invested in other data protection mechanisms including cyber-security, fraud and scams.

Assisting in a crisis

The strategy outlines how government access to non-government data can assist with economic, social, health and environmental crises. One example cited is the bushfires of 2019-20, another is the response to COVID-19. Banks supported the Australian Government's economic response to COVID-19 by providing data on loan deferrals through APRA, as well as expenditure directly to the ABS. This type of support comes at a cost to banks: providing resources to establish the data architecture through which data is submitted, as well as apply governance across it.

APRA is currently consulting on its directions for data collections which outlines it's move from static form-based reporting to dynamic datasets. There is benefit in providing data in ways which can be flexibly examined and immediately available in times of crisis. These data collections are intended to be crisis-neutral, given many data collections can be based on the data needs of the last crisis, however as we know from history, often crises can be 'black swan' events which are not planned for.

Some ways that governments use bank data during crises raise questions about the applicability of the Privacy Act. An exception to the Privacy Act has been used developed for these purposes, however it would be useful if there was a longer-term determination made with the Office of the Australian Information Commission (**OAIC**) possibly through an affirmative confirmation or a carve out in privacy law as under Article 6 1(e) of General Data Protection Regulation (**GDPR**), so that future requests are entirely exempt from the Privacy Act.

Sharing government data

While banks have shared their data with government and non-government recipients for the benefit of customer, social, health and economic outcomes, banks do not have the equivalent access to government data for these same purposes. ABA members are supportive of the government's intentions to break down unnecessary barriers to enable the private sector to get more value out of Australian Government data assets.

With customer consent, as well as appropriate privacy controls, banks accessing data held by government data could:

- enhance consumer choice and potentially increase the availability of credit to responsible borrowers,
- assist firms to satisfy regulatory requirements, including responsible lending,
- improve credit management and the efficiency of financial market risk pricing, and
- facilitate competition in the financial sector by access to validated information on customers thereby simplifying the credit origination process and enabling customers to more easily assess their viability with different lenders.

An immediate action that could be taken by Government is enabling citizens to share their Australian Tax Office (ATO) data. To simplify and expedite loan applications, the ATO could allow customers and small businesses to consent to sharing specific financial information with credit providers. For example, data relating to income, cash flow and negative gearing arrangements which is held by the ATO. This could be made available to credit providers through the CDR platform. ATO data could also be used to verify tax information and streamline applications for government schemes, such as the First Home Loan Deposit scheme, HomeBuilder scheme, Small and Medium Enterprise Recovery Loan scheme.

A second example of how bank customers would benefit from banks accessing their data held by government agencies is business customer information held by the Australian Securities and Investments Commission (**ASIC**). Again, with customer consent and potentially within the CDR regime, banks would be able to verify company details including Australian Business Numbers, Australian Company Numbers, and standardised industry codes. This would benefit directors opening bank accounts by streamlining processes and likely resulting in more timely decision-making, including for the purposes of credit decisions.

Trust and protection

A modern economy is built on insights generated from data. But not all data is created equal, and nor does access to all available data immediately generate positive social and economic outcomes. The Government's consultation on the data security action plan recognises that misuse or compromise of data can harm national security interests, and weaknesses can come from government (at all levels) as well as the private sector. We support a data security policy that enables public and private sectors to take a strategic view of how to protect customer data and how data can be used – including movement across national borders.

Data sharing between private and public sectors needs to be supported by a clear framework as to its purpose and how it is to be used. The framework for any data sharing exercise should, without being unduly complicated or onerous, include explanations as to the priority of the data, the intermediary which will hold the data, the end users of the data, and the legislative frameworks which govern the data.

Data security

Australians hold a high level of trust in the banks to manage their data, relative to other industries[1]. Customers' expectations are that Bank's keep their information secure at all times. Data security at banks can be put at risk where there are inconsistent data security or privacy laws, and/or inconsistent data security practices within government. ABA members welcome the commitment by government of providing integrated data environments with secure access environments.

Data breaches in recent years have resulted in sensitive bank information being made public. For example, a breach at the Reserve Bank of New Zealand resulted in the release of sensitive board

[1] Representative sample surveys of Australians conducted by academics at the Australian National University and by the private company Frollo indicate that customers trust banks to hold their data securely relative to other industries. Biddle, N., Edwards, B., Gray, M., Hiscox, M., McEachern, S. & Sollis, K. (2020) *Data trust and data privacy in the COVID-19 period,* ANU Centre for Social Research and Methods; Frollo (2022) *Open Banking: The Consumer Perspective,* Frollo.

papers. In Australia, a data breach at ASIC resulted in credit licence applications being viewed. While no information contained in the applications was read or downloaded and only file names were seen, this illustrates the need for vigilance by government, and all parties, when acquiring and storing data. In context of the data security action plan, banks are calling for Government policy to have the objective of protecting data commensurate with sensitivity and harm, and to implement this policy across all levels of government as well as the private sector.

Public sector agencies often have a mandate to require data reporting from individuals and businesses. Banks need assurance that the same level of protection will be maintained when sharing customer data with government agencies. Given the advancements made in sophisticated data mining techniques, even where banks anonymise customer data there is still the possibility that it may be made identifiable. These weaknesses can affect the security of bank data. While data collected from banks under Section 56 of the APRA Act is exempt from the DAT Bill there is a risk that other bank data collected by government may be shared with third parties under the DAT Bill.

Banks are looking to government to ensure that there are appropriate data management techniques to avoid any risks to customer data when shared with third parties (whether under the Bill or otherwise). Two areas of action are adopting consistent and rigorous policies about who can access specific data based on roles and responsibilities (going beyond security classifications) and enhanced requirements to review the data security capability and policies of entities that receive data and information from public sector entities.

Data governance

Government oversight of industry data management practices is an expected part of industry regulation. There is currently some government guidance on best practice data management, including APRA's detailed prudential practice guide CPG 235 which outlines expectations around managing data risk. Given banks have adopted robust governance processes for the use of technology, including artificial intelligence (**AI**), any new guidance should be developed with consideration of the skills and knowledge already existing within the industry. Regulation should be principles based rather than technique specific, as technical guidance may soon be obsolete given the fast-paced evolution of the technology. A supervisory framework should include governance of capability of management and risk controls that are in place.

Customer consent

An essential component of sharing customer data is consent. This is typically only needed when sharing customer-level, or account-level data. Data that is combined from a number of customers (aggregated data) and from which individual customer information cannot be identified does not generally require consent. In some circumstances, however, the use of data to generate such aggregated data sets may require consent. Clear, communicable consumer consent needs to be at the heart of data sharing arrangements.

Data retention

The Australian data strategy notes that there are some accountabilities for data retention, however these relate to the retention of data by government agencies. There is no clear guidance for non-agency holders of data as to methods of storing data, or periods for which it should be stored. Further, different jurisdictions have different expectations of how long data should be stored. Therefore, banks currently have their own practices around data retention which are not necessarily aligned with each other, nor with data storage practices in other industries. These practices draw upon a mixture of legislation and regulation which is up to banks to interpret.

Enabling data use

The final aspect for consideration of the strategy is the need to plan for continual change. Any strategy that is developed for today's world might be outdated within just a few years. It is possible that data technology, analytical techniques and uses might evolve more rapidly than the strategy. We are already

seeing the development of digital currencies, the Internet of Things, and the metaverse. Therefore, the world of data, and how it interacts with banking services may look very different in five or ten years.

Legislative simplification

The Australian data policy landscape is complex, with a number of overlapping regulatory regimes with good intentions but that can, at times, be at odds with each other, or that do not have sufficient scope to unlock the value of the regime.

For example, under the *Privacy Act,* entities that do not hold an Australian Credit Licence (**ACL**) are restricted from exchanging repayment history information through the comprehensive credit reporting (**CCR)** regime. This limitation means that entities, such as telecommunications companies and Buy Now Pay Later (**BNPL**) firms are unable to share credit information. In turn, this limits the ability for the CCR regime to meet its goal of giving lenders access to a deeper, richer set of data to better assess a borrower's true credit position, ability to repay a loan, and avoid any unfeasible accumulation of debt.

Expanding CCR participants by removing the requirement to hold an ACL will allow the regime to better work by allowing all participants to exchange detailed account level data. Under this operating model, the Principals of Reciprocity and Data Exchange would specify that entities can only receive consumer credit information up to the same level at which they are willing to supply information (i.e., entities that do not report repayment history information cannot receive it). This will be an incentive for an increasing number of entities to participate in the regime over time.

Skillsets needed for a data economy

While it is difficult to plan for what has not yet developed, the Australian Government needs to consider the evolving nature of data when considering future labour markets and skill requirements. As the world of data becomes larger, more workers are going to be needed to meet the demand. ABA members are having difficulty finding skilled workers to meet the current data projects being implemented by government. This is partly because staff are being poached by other industries who are implementing the same types of data projects as the banking industry. It is further exacerbated by low levels of immigration resulting in fewer skilled staff to bolster the current workforce.

Further, the right skillsets are needed to unlock the potential for government and industry data. As the strategy rightfully notes, up to 80% of the work done with data is on sourcing, collating and cleaning. This necessitates a labour force with the appropriate skillsets to conduct these activities. While there are many tertiary level qualifications in analytics, there is not the equivalent in data governance and management.

What offerings do exist in data governance and management tend to focus on the management of the data of a single business. However, there is increased complexity when integrating and managing the data of multiple businesses. The current exercise run by APRA to develop a comprehensive credit collection is illustrative of this complexity. ABA is supportive of APRA's approach to co-developing the collection with the banking industry in order to develop a data architecture which corresponds to the way banks currently hold and store data.

Learning from the experience of other jurisdictions

As the Australian Government continues to support a data-oriented economy, we encourage the Department of Prime Minister and Cabinet to examine the data strategies of other nations leading the way in these endeavours and who have second and sometimes third iterations of national data strategies. These include Singapore, New Zealand, the United Kingdom, the European Union and the United States of America. These strategies outline not only current activities that are underway, as is done in the Australian Data Strategy, but also a future vision and the activities that will be undertaken to achieve that vision.