ID Exchange Pty Limited
Stone & Chalk FinTech Incubator
Wynyard Green
11 York Street
Sydney NSW 2000 Australia
E: advisory@idexchange.me
M: +61 (0)400 770 147

www.idexchange.me

Mr Daniel McAuliffe
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600

September 10, 2018

Dear Mr McAuliffe

Consumer Data Right – response to request for consultation

We welcome the opportunity to contribute to this consultation process.

Over the past three years we have participated in a number of government and industry-initiated inquiries and forums relating to the use of data in conjunction with new technologies and the corresponding need for policy and law reform to support information innovation and competition.

These have included the Senate Inquiry on the National Innovation and Science Agenda, the Productivity Commission's Review into Data Availability and Use and the Treasurer's Open Banking Review.

About ID Exchange and digi.me

ID Exchange is an Australian company that was established in 2012. We develop privacy enhancing technologies (PETs) and digital rights management solutions to assist consumers to protect and mobilise their data for their benefit. Our technologies provide consumers with the means to control and manage their data using methods such as unified opt in and opt out consent controls. Further information about ID Exchange can be found at https://idexchange.me.

In 2017 ID Exchange partnered with digi.me.

digi.me is a UK-based enterprise. Since 2009 we have developed and deployed technologies that provide consumers with enhanced levels of control over their data that enable them to exercise their information privacy rights more effectively. Digi.me technologies are designed to promote the trusted handling of personal data – in a sector where trust has declined because of dubious data practices adopted within the tech industry in recent years.

digi.me accomplishes this using a unique information architecture that relies on linkages and synchronous data handling. digi.me does not see, touch or hold data. This minimises security risk and provides consumers with choice about data storage and transfer options.

Our business model is commercially attractive. Transaction costs for businesses wishing to access data is priced universally at USD$0.10c per source transaction, per user, per annum, with an annual maximum cap at USD$3.00 per user, per annum.

digi.me is compliant with all existing and forthcoming data privacy legislation, including the EU's *General Data Protection Regulation* (GDPR) and the *California Consumer Privacy Act 2018*.

Our collaboration with ID Exchange is an example of the type of new entrant into the market for personal data that the CDR is intended to promote. Further information about digi.me, including detail of the software and Apps we have successfully deployed, can be found at https://digi.me.

Submission summary

We support the CDR but we do not consider that it meets the policy objectives it is designed to address. We understand these objectives to be:

- promoting competition;
- promoting innovation;
- enabling the development of new businesses and business models;
- providing consumers with efficient and convenient access to their data; and
- ensuring that these rights are accompanied by strong privacy and security protections.

The focus of our submission

To better meet these policy objectives, we argue that the CDR should be amended to:

- Remove sectorial barriers so that it applies across the whole of the private sector
- Reduce its multiple layers of regulatory complexity
- Provide a clear and timely approval mechanism to ensure that accreditation processes do not become mired in excessive regulatory burdens and extensive, costly delays
- Provide more robust controls over regulatory discretionary decision-making
- Include an overarching system of governance that is independent of the Minister and the Commonwealth public sector which has responsibility for overseeing the implementation and operation of the CDR *as a whole*
- Narrow the scope of the data covered by the CDR so that it does not cover 'value added' data
- Provide better privacy protection, noting that multiple, overlapping privacy safeguards are likely to produce confusion, rather than better privacy protection
- Ensure that security safeguards are proportionate and 'fit for purpose' having regard to the fact that security risk postures within the CDR ecosystem will be variable

The international environment

The CDR is being developed in an environment where the EU has already established and implemented data portability across all of its economic sectors under Article 20 of the *General Data Protection Regulation* (GDPR). Because information enterprises operate across international boundaries, many Australian and other businesses have already taken steps to comply with it. The GDPR is a 'light touch' data portability regime. It establishes data portability in 206 words. The CDR Bill establishes a more limited and complex right in 16,456 words.

The GDPR is an international benchmark. Australia's trading partners are actively considering it as a model for economic and information reform. Its relative simplicity compared to the CDR is likely to appeal to many. This simplicity combined with the relatively frictionless information environment it creates places Australian enterprises subject to the CDR at a regulatory disadvantage.

The GDPR's data portability right is not hedged by the complex regulatory system that the CDR establishes. For example, there has been no need to establish a Data Standards Body (DSB). Technical data transfer issues have been covered succinctly by the Article 29 Data Protection Working Party's (now the European Data Protection Board) *Guidelines on the right to data portability.*

Another implementation of data portability is the UK's open banking system which appears to have had a substantial impact on the shape of the CDR. However, UK open banking and the Australian CDR cannot be validly compared. UK open banking is designed to facilitate payments and remittances and therefore is required to encompass a broader range of regulatory requirements. The CDR does not.

Implementation of the UK's open banking system has proven to be challenging. When it commenced, only a few businesses had received the necessary regulatory approvals. There is currently a significant regulatory backlog. Compliance costs, which typically amount to £20,000.00 have deterred many and delayed the realisation of benefits.

It is important for Treasury to take account of the international context before finalising its work on the CDR. The CDR will not deliver on its aims when information businesses have the opportunity to locate their operations in jurisdictions that have developed more straightforward regulatory frameworks, where compliance costs are much lower and that also protect privacy and security to a standard that significantly improves on equivalent Australian protections.

Commentary

One of the main difficulties we have had in attempting to assess the potential impact of the CDR legislation on objectives such as introducing additional competition in the financial services and other markets is that it is framework legislation. Most of the detail that will have a major impact on *how* it will operate, the obligations it will impose and the regulatory burdens it establishes are left to the Minister, the ACCC and a range of new entities.

This submission is being made in advance of any of these key details. For example, the ACCC will not be publishing its rules framework – a key element of the new framework – until *after* the closing date for submissions on the CDR Bill. This is an unsuitable approach for such an important piece of information reform. Importantly it is an example of some of our main concerns about the CDR that our outlined below.

Sectoral barriers

The CDR Bill is intended to apply sector by sector over an indeterminate time period. That said, there is no guarantee that it will apply to the *whole* of any particular sector as its application will involve the Minister determining *who* it applies to and from *when* it applies (cl 56AC(2)).

The reality is that the CDR will *not* be implemented on a sectoral basis. It will apply, organisation by designated organisation within designated sectors. Each decision to apply it to an organisation will involve an exercise of discretionary decision-making by the Treasurer. Each such decision is an opportunity for information incumbents in the financial sector to argue special circumstances and to challenge the decision-making process in the courts.

This incremental approach means that the benefits of the CDR will be delayed. It also means that information incumbents will have a disproportionate influence – through lobbying and special pleading – over a designation process that is not transparent, public or accountable.

The designation process requires a range of matters to be taken into account (cl 56AD) and requires consultation with the ACCC, the OAIC and 'any person or body prescribed by the regulations.,'(cl 56AD(2)(b)). It is unclear to us how this regulation making process will be undertaken and how or why the privileged status of these persons will be determined.

Our preferred approach is for the sectoral limitations on the CDR to be removed so that it applies to all of the private sector from the beginning. This will mean that:

- its competitive and innovation dividends will be realised sooner;
- the likelihood that information incumbents delaying its implementation will be reduced: and
- sectoral application will be transparent and accountable.

Complexity

As framework legislation, the CDR Bill leaves too many decisions that will have the effect of legislation to be made by too many entities. These include the Minister, the ACCC, the OAIC, the Data Recipient Accreditor (DRA), the Accreditation Registrar (AR) and the DSB.

All of these entities or bodies have substantial law and rule making powers. This division of functions and responsibilities creates an opaque decision-making matrix. It is a complex, costly and burdensome implementation of a simple policy – enabling consumers to access their personal information in digital form and/or to direct that it be supplied to a third party.

This complexity can be removed by:

- applying the CDR to the entire private sector from the start (which obviates the need for sectoral designation)
- legislating for accreditation standards (removing the need for the DRA)
- simplifying the multiple layers of privacy protection so that one set of principles apply (removing the need for the ACCC to develop consumer data rules)
- requiring the DSB to publish data standards before the CDR comes into effect or, alternatively, adopting the European Data Protection Board's approach.

Overall, the lack of clarity of the regulatory framework undermines its clarity and its ability to efficiently address its policy objectives.

Attached as Appendixes are diagrams that set out a simpler, more straightforward approach to implementing data portability.

The need for controls over discretionary decisions

Although the CDR Bill confers powers and functions on a number of existing and new entities, it says nothing – except in relation to the Minister's sectoral designation powers (cl 56AD(1)(a)) – about how these powers are to be exercised, the principles that should guide and limit discretionary decision-making and the matters to which decision-makers should otherwise have regard.

Although the need for such guidance would be reduced if our recommendations about simplifying the CDR Bill are adopted, for each of the entities that are involved in CDR decision-making, the Bill should provide clarity about their roles and responsibilities and how they exercise their discretionary powers.

The entities established under the CDR legislation are simply offices within Treasury. This means that they are accountable to and report to Treasury: they do not operate on an arm's length basis. We question the desirability of this structure. Essentially, entities such as the DRA, DSB and the AR have no independence and will be subject to Treasury's direction. Although this might be an acceptable arrangement in some parts of the financial sector, it is not appropriate for the conferral and enforcement of fundamental rights such as privacy.

We also question the conferral of law-making powers on the ACCC. For example, under cl 56BA the ACCC is responsible for establishing the consumer data rules. These will have a major impact on the operationalisation of the CDR. At the same time, the ACCC will have jurisdiction over the enforcement of the rules that it has made. This is an inappropriate mixing of law-making and law enforcement functions.

Governance

The CDR Bill establishes new entities with new powers and functions and confers new functions on existing agencies, but no one is responsible for overseeing the CDR scheme *as a whole.* The Bill does not establish an independent body tasked with overseeing and monitoring the multiple 'moving parts' of the CDR scheme. There is no mechanism to measure its effectiveness or to investigate and report on issues and problems that may arise.

We recommend that such a body be established as an independent statutory office.

CDR data scope

Under cl 56AF, CDR data covers information that is designated as being CDR data, data that is directly or indirectly derived from CDR data (cl 56AF (2)), and data that is associated with other CDR data (cl 56AF(3)).

Derived and associated data should not be included. Such data will be the 'value added' data that is produced by data holders through both combining it with other data, producing insights based on using advanced data analytics or both. The inclusion of such data within the CDR is an innovation disincentive for data holders and conflicts with the CDR's policy objectives. It may also be an invalid exercise of the Commonwealth's legislative powers under s 51(xxxi) of the Constitution.

Multiple layers of privacy protection

Although we support the CDR's objectives of providing strong levels of privacy protection for consumers, we question whether a combination of the CDR's unspecified consumer data rules, the Privacy safeguards set out in Division 5 and the APPs is the best approach.

Although we welcome stronger privacy protections, particularly an extended definition of personal information and the potential for a more calibrated approach to consent (which depends on the ACCC) it is difficult to understand the value of this multi-tiered approach to privacy., A better approach would be to rely on a single set of principles – the APPs – suitably reformed to be consistent with GDPR-level protections. We note that data portability has been implemented in the EU, *with* stronger privacy protections but without the need for three different levels of privacy principles.

We also believe that a multi-tiered approach to privacy protection compounds the cost of implementing the CDR. The organisations that will be most affected are new market entrants and those without the highly skilled legal and other resources that will be necessary to navigate the complexity of the CDR.

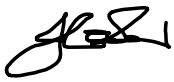
Security

We support the need for the CDR to be accompanied by robust security protection. That said, its approach to security should be sufficiently flexible to recognise that security risk across the CDR ecosystem will vary significantly. A 'one size fits all' approach is neither necessary nor desirable. For example, compliance with a standard such as ISO 27001 is suitable for the risk posture of financial institutions but is unlikely to suitably reflect the risk posture of other, new participants and intermediaries such as ID Exchange and digi.me who will hold no data.

Overall, we are convinced that the CDR is a key opportunity for reform that can promote digital transformation enhancing the Australian economy to realise the benefits of information reform and that provides a solid trust foundation by establishing strong privacy and security safeguards. We believe that the CDR needs to be rethought to achieve these objectives.

Please feel free to contact us for any further clarification, assistance or continued input about this submission.

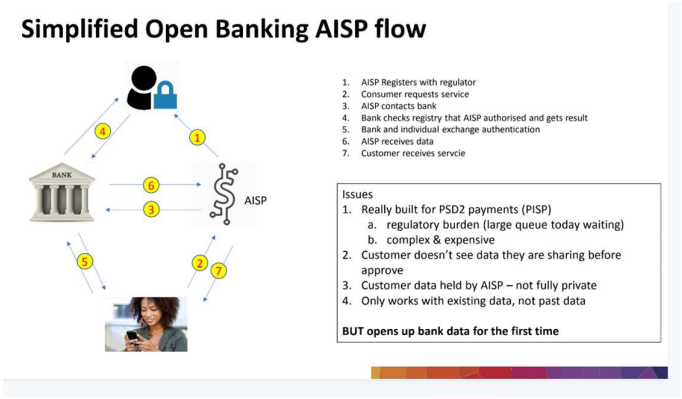
Kind regards,

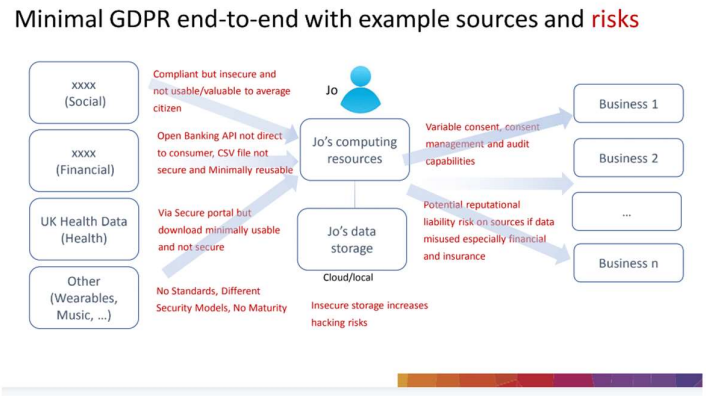


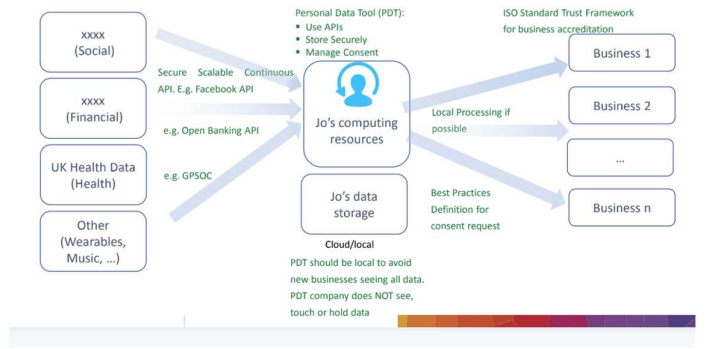
Joanne Cooper
Founder, Managing Director
ID Exchange Pty. Ltd.

In partnership with digi.me Ltd (UK)

Appendix 1







What does this mean for Australia?

A collaboration between one UK business and two Australian businesses to bring the lessons learnt from PSD2/Open Banking and GDPR to Australia to implement Open Banking / Consumer Data Right today

- For banking
- And for other consumer data immediately too