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

23rd January 2019

Dear Mr McAuliffe

Privacy Impact Assessment - Consumer Data Right – stakeholder review

ID Exchange in partnership with digi.me Ltd UK is pleased as an industry stakeholder to provide continued feedback on the forming Consumer Data Right (CDR) Bill and the CDR Privacy Impact Assessment (PIA) draft released for industry input and review.

In reviewing the document, we request the opportunity to draw reference to our prior CDR and Open Banking submissions and direct discussions whereas we have stated our continued support of the CDR Bill but believe there remains elements within the CDR's approach which does not speak to primary objectives to which this Bill 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.

We note within the first paragraph of the CDR PIA draft (cut in to this response below with our simple mark-up in Red) that we feel the PIA inadvertently fails to connect with the central theme whereas the CDR is designed to be structured to provide customers choice, competition and confidence via increased data controls of an individual's personal information to drive innovation market competition and economic opportunity.

Executive Summary

Consumer Data Right background

The Consumer Data Right (CDR) provides individuals and businesses with a right to access data and regain a copy of the data relating to them held by businesses (for example, raw bank transaction data); or to authorise secure access to this data by accredited third parties. The right does not enable businesses that hold data to transfer or use data without the customer's consent.

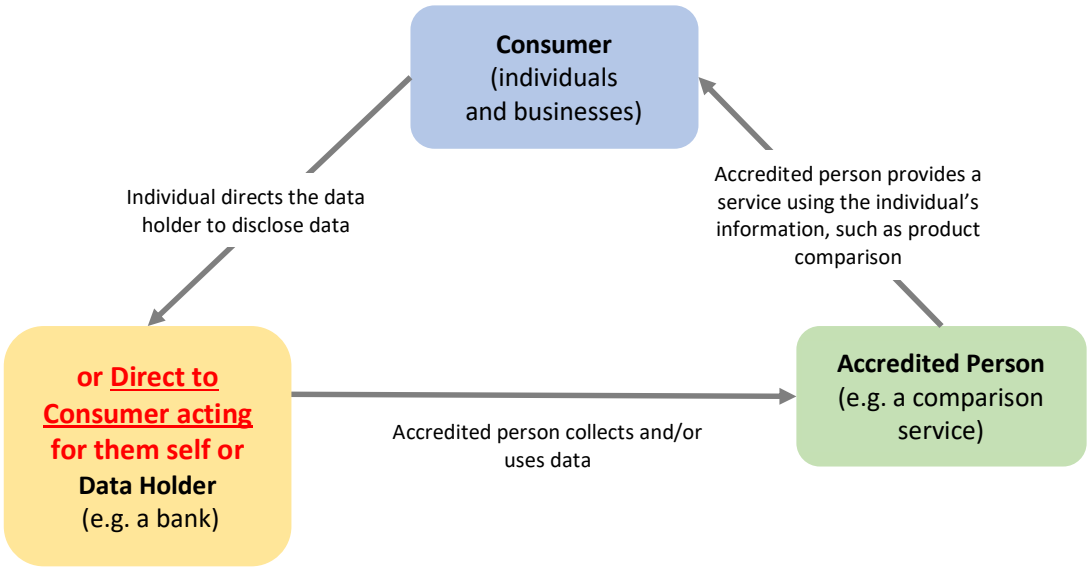
This suggested correction indicates that consumers first and foremost have the right to access data directly if required or via an (approved) intermediary, which means the user can direct data back to themselves so "over time" the individual becomes the comprehensive data holder (multi -sector) enabling the overarching goal of full consumer centricity.

It also appears in our view that perhaps due to the markets perception of todays traditional technologies the CDR PIA appears to have represented providing data **direct to customer** is an afterthought and the diagrams do not simply articulate a **parallel option** within the model to provide the customer it's right to retain a direct electronic copy and onward control of their personal data which via innovative new platforms can be securely obtained via API's plus enable the new paradigm of "private sharing" which means the data never leaves the consumers control and is accessed via consent controls and algorithms coming to the consumers specific data sets.

Whilst this may be a primary objective of the understood intermediaries – it would also benefit from being clearly stated that intermediaries will differ in their business models.

Not to labour on this point we have provided key samples below from the CDR PIA draft with suggested changes which are again indicated in red:

Primary framework diagram



CDR - Mapping of personal information flows

Simple Consumer Data Right model

An example of how the CDR may function is outlined below. Note that the personal information involved in flows under the CDR is limited to personal information that has been designated as subject to the CDR in a sector designation instrument – this example uses banking data. This example sets out a simple use of the CDR with only three parties: the individual, a data holder and a data recipient.

The diagram below illustrates this model.

Stage 1: Individual engages with data recipient

Naomi is considering changing to a different credit card. She wants to compare her current credit card to other options on the market and engages a comparison website, BetterDeals (the data recipient).

Stage 1b : Individual engages as the data recipient

Naomi is considering changing to a different credit card. She wants to compare her current credit card to other options on the market and engages a comparison website, BetterDeals who wish to propose the best credit card options tailored for Naomi. To do this BetterDeals requests Naomi (as the direct data recipient) to downloads their App which is integrated with a personal data sharing platform called All-data (aka digi.me). This allows with consent BetterDeals to deploy an algorithm to analyse several of Naomi's transactional and social accounts and her financial data. Naomi downloads the BetterDeals App which includes the All-data App allowing her to easily connect via an API to her Bank(s) and Social media accounts after successful ID Verification/Authorisation. In the background the Banks system sync's All-data via an ACCC accredited intermediary "clearing house" to compliantly port her transactional data which is encrypted, directly back to her. The All-data App requests her to self-store her personal data into her choice of Cloud storage service or device (decentralised). The BetterDeals App sends a call to Naomi's All-data App and asks for access to both finance transactions and social data directly from Naomi's private data store via a detailed, transparent, specific consent process which is CDR/GDPR compliant and can activate the right of erasure. As Naomi's All-data App has automatically normalised all her returned data it's searchable and interoperable and is provided to Naomi a rich digital UX format. Naomi grants consent to the BetterDeals App to access data which runs an algorithm over her data to obtain a result/score, so no data has been duplicated by BetterDeals or left Naomi's control and her privacy is maintained, Naomi freely shares access and trusts this new form of "Private Sharing". Better still Naomi can view and search across all her data to personally derive her own personal data insights. In instances where the BetterDeals algorithm needs to take a copy of the minimum subset of Naomi's personal data it will request this from Naomi during a fully transparent and informed consent process. The consent receipt is time stamped so if data is taken by the BetterDeal's App it is set for auto erasure in a prescribed time period.

As the CDR's PIA draft appears to have fundamentally overlooked that the individual can receive the data directly, even though GDPR Article 20 is referenced which is exactly that case and even though the draft does on occasion (as on page 11) state that "enable a consumer to: receive a copy of their consumer data".

The diagram on page 4 shows simplified exchange diagram (in your words) and then page 5 says other participants might add more complexity. Yet the direct to Consumer option is the simplest routing of all as only two boxes, Data Holder and Consumer.

Why this matters? Because the CDR is to empower consumer data controls so direct to Consumer (most probably with an intermediary who will deal with privacy, security and consent) must be a major option (and the consumer then on shares data). This is simpler and hence the CDR could be applied to all sectors immediately rather than Banking first.

A holistic and harmonised approach mitigates sector by sector complexity which we strongly believe will delay economic benefits at best, and digital transformation opportunities will be lost as other nations build systems (that will work in Australia) without such limitations and complexity.

Our argument is based on:

1. Simplicity
2. Australia leading the world and benefiting economically quickly
3. The individual being the best (& most private) aggregation point – and this maximising future innovation

With the clear recommendation of remove all complexity in the system

1. Data made available, through INFORMED consent (which needs to be clarified to the extent that this is realist) via a well formed API
2. All sectors

In our prior CDR submission, we also cited the issues and complexities that stipulating a "sectoral approach" will bring. We again restate our view that sectoral limitations on the CDR be removed and that the CDR immediately applies to all 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.

As our partner digi.me has built a model where we believe that through the provision of giving data back to the user it is possible to create a change in businesses who are depended on the free model, where the user does not pay directly for services (Facebook, Twitter, free-to-air advertising TV) however the same model also suggest that "giving" data back to user WILL NOT create the change of behaviour of those companies who have a direct business where the consumer pays for a product of service.

Therefore, the planned roll out is unlikely in our view to deliver the objectives of

- 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.

Having read the papers in full, we believe that there should be a nomenclature used throughout the document that describes the type of privacy which the authors talk about at various points – as the generic word in being applied in several contexts which means there is a high degree of ambiguity in what privacy is being referred to at any stage, our suggestion is the following as a start:

a. Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records;
b. Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches;
c. Privacy of communications, which covers the security and privacy of mail, telephones, email and other forms of communication; and
d. Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.
e. Private privacy: space, mind and interactions
f. Relationship privacy: consent and protection by association
g. Consent privacy: who and what you have shared

We believe that the document and supporting recommendation could do with another iteration on consent and consent management as this becomes a critical factor to create change in behaviour and reporting.

The importance of regulatory initiatives across the globe is that models that stand to gain traction must be created with the mindset to avoid fragmented ecosystems and standards frameworks which will be a barrier to data portability due to complexities that negate interoperability instead of staging the future of harmonised data sharing across industry and international borders.

Our approach was that a sectoral view to CDR standards cements a fragmented framework from the outset and should be avoided as it will slow and hinder innovation and create an unnecessary impedance to economic trade stimulus.

We refer to our Asia Pacific neighbours like Singapore and Thailand who within their Payment Systems have geared frameworks towards systemic efficiency whilst still ensuring consumers are protected with a view to interoperability through data portability.

Regulators that effectively balance the need for data privacy and protection to mitigate payments risk required to leverage digital payments volumes with the introduction of light touch regulation for data protection and security will set the transformation pace and with success will seek to target our citizens.

As an Australian company operating in an open and competitive market, today we can demonstrate advanced systems architected for private personal data sharing whereas the individual has the right to full agency of their data, i.e. processing of data done on the individual device rather than data being sent to yet another server. This feature alone is probably the single biggest privacy risk mitigator.

This allows us to implement the simplest and, in our view, most secure route for data sharing with privacy and consent (GDPR compliant) and it's ready now.

Technology that securely enables direct to the individual will always be the best – both for privacy and enabling a super-set of data to be collected to spur innovation. This decentralised model is security and privacy by design and ready for "plug and play" integration for 86% of Australia's Banks.

The platform is designed to meet tier one banking compliance and liability/risk requirements with social data streams already integrated and the ability to immediately integrate via API's interoperable Telco, Energy and Health data under a single data normalisation and ontology approach.

As an Australian technology firm working amidst global thought leadership to assert "human and consumer centricity outcomes" by partnering with world leaders like Julian Ranger, Chairman of digi.me we have answered the Governments call to innovative, collaborate and leverage trade opportunities to provide advantage encouraged through Trade delegations and programs like the Australian British Chamber of Commerce Aust/UK FinTech Bridge to which we have been an active participant.

We have worked hard to openly and fairly to partake in market competition by prioritising infrastructure readiness with both social and Open Banking API's and consumer data flows available allowing the Australian market to participate and demonstrate leadership through early roll-out of cost-effective platforms that will indeed enable the CDR.

We are strengthened in our advanced approach by statements from CEO's from Apple and Microsoft driving the narrative towards consumer centric data controls that elevate digi.me's early position. See: https://www.washingtonpost.com/world/europe/apples-tim-cook-delivers-searing-critique-of-silicon-valley/2018/10/24/5adaa586-d6dd-11e8-8384-bcc5492fef49_story.html?utm_term=.69e56a6861ca

Whilst outside of the current mandate this framework does have an effect and implication on corporate governance. We believe that it is critical that this is not lost as the impact of the CDR is not covered in any existing rules, guidelines, best practices or legal cases so it should at least offer some insights into the new responsibilities that directors will face.

As such and in the spirit of innovation to truly advance Australia's place in the data economy we call for our input to be taken onboard and incorporated to encapsulate the best outcomes for Country, Business and Consumers alike. We continue to offer executive access to reach outcomes that will ultimately showcase the CDR's objectives.

Finally, we wish to reinforce that we very much welcome the nature of open competition in the data economy and trust that this will not be limited to outdated or traditional models which sideline emerging platforms.

Kind regards,

Joanne Cooper
Managing Director
ID Exchange Pty Limited
Australia & New Zealand Representative for digi.me Limited.

Privacy Power Protection

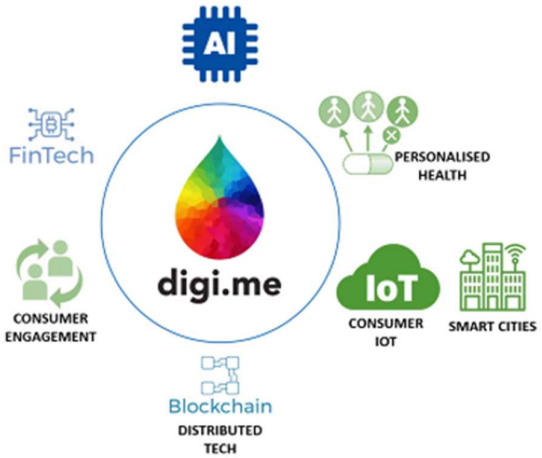
Supporting diagrams detailing the digi.me personal data sharing and interoperability platform.

Enabling an ecosystem win with the emergence of new decentralised consumer centric approaches:

- Do more with data*
- Privacy assurance drives trusted interactions
- Interoperability promotes new services
- Consumer agency of data provides self-governed insights
- Choice and value exchange promote economic stimulus
- Complex interwoven tech stack moves to pervasive delivery
- Big win for all as the model drives confidence for Government, Enterprise, SME's and Consumer

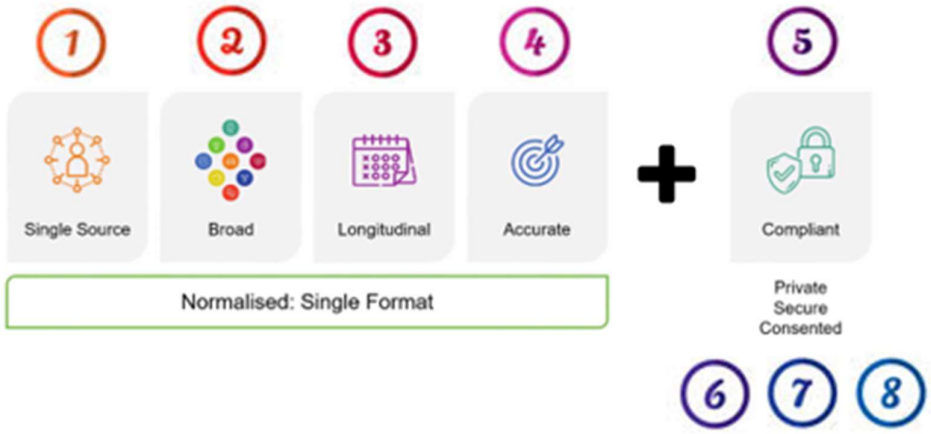
**Shift perception into the new personal internet with the understanding Privacy will enable you to do more.*

The data economy has a dependency on the interoperability of data, digi.me resolves this by allowing the consumer to be the control point with full agency of self-stored personal data.

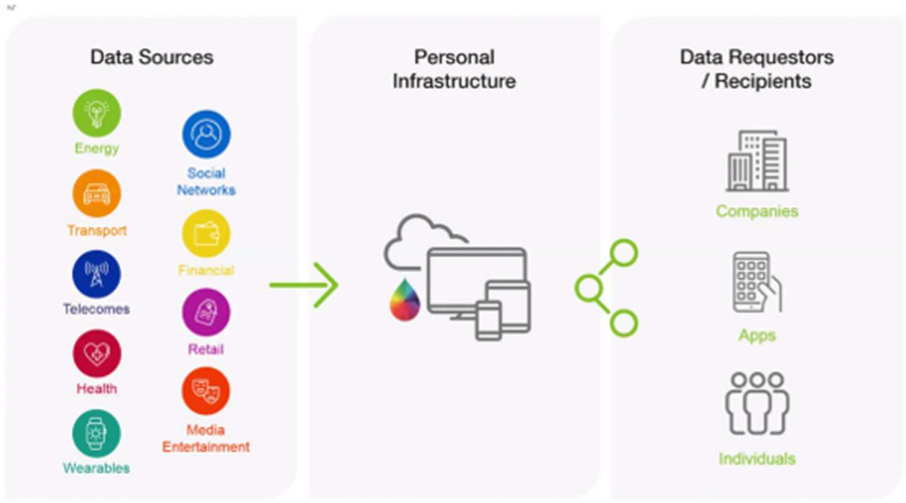


digi.me is a ***decentralised personal data solution*** enabling developers to have access to ***rich consented personal data*** in minutes using digi.me's ***consent access system*** and ***developer friendly SDKs***

Eight elements are required to achieve rich data interactions within the data economy:



How digi.me data sharing works:



Samples of supporting reference material:

Case study | Cntrl Shift – techUK
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/755219/Data_Mobility_report.pdf

Video tutorials | https://digi.me/video

Most recent award | https://blog.digi.me/2018/11/21/digi-me-named-as-one-of-europes-top-100-digital-pioneers/

Australian Open Banking Hackathon | https://www.cso.com.au/article/648845/boutiq-scoops-top-prize-new-south-wales-spark-festival-digi-spark-hackathon/

Commitment to RegTech Innovation | https://www.technologydecisions.com.au/content/it-management/news/id-exchange-and-digi-me-open-innovation-hub-791851339

Government adoption | https://govinsider.asia/digital-gov/iceland-health-data-app-digi-me/