



# Inquiry into Future Directions for the Consumer Data Right

April 2020

# Contents

<b>Executive Summary</b>	3
<b>Contextualising the Consumer Data Right opportunity</b>	4
<b>Consent Management: The critical layer we need to get right</b>	6
<b>Expanding access: A controlled CDR-utility layer for SMEs/startups</b>	9
<b>International developments &amp; harmonisation - Future Proofing Australia's Consumer Data Right</b>	10
<b>Driving efficiency and productivity through a centralised Data Agency</b>	15
<b>Consumer Protection</b>	18
<b>About Data Republic</b>	19
<b>Concluding Note</b>	19
<b>APPENDIX:</b>	20
<b>Insights from Data Republic Market Research into Consent Management Models</b>	20

## Executive Summary

Data Republic welcomes the opportunity to make a submission to the **Inquiry into Future Directions for the Consumer Data Right**.

An example of a globally scaling startup, at Data Republic we're on a mission to unlock data-driven innovation through safe data sharing. We believe that by enabling governed data sharing, wiser decisions can be made and better outcomes delivered for individuals, businesses, and society.

Over the past four years, Data Republic has worked with industry and government across Australia, Singapore and the United States to develop a best-practice technology platform for the secure governance, licensing orchestration and protection of privacy when sharing data between organisations. In that time, we've grown our team by 6X, expanded to 2 additional markets and accessed the R&D tax incentive.

Our submission shares insights from a leading global enterprise software company, building innovative technology to address data and privacy risks for consumers and business, while trying to navigate Australia's fragmented policy and regulatory approach to both the data economy and digital ecosystem as a whole.

Key topics addressed in our submission include:

- The limitations the current CDR approach places on the potential of Australia's data economy
- The need for an expanded, technology-first approach to consent management within CDR to boost innovation and competition
- Recommendations for linkages between CDR and existing systems/ infrastructure

Thank you for your consideration,



**Danny Gilligan,**

CoFounder & CEO, Data Republic

## 1. Contextualising the Consumer Data Right opportunity

Data Republic believes that data is the single biggest lever for micro-economic and social reform in the next two decades. Consequently, we see an opportunity for Australia's emerging data economy to rapidly develop into a material new sector of the economy across that period.

We define the data economy as the trade in data between organisations and/or governments, domestically or internationally, and the derivative data products (algorithms, insights, applications, services) that arise from that previously unavailable flow of data. The data economy is comprised of organisations and governments that are able to provide personalisation of services through data insights as well as develop data-driven solutions to existing and emerging problems. It deals with productivity issues in the private sector (personalisation, risk, identity, supply chain efficiency, decisioning, development of artificial intelligence applications) and social reform issues across the public sector (policy reform, allocation of resources, programme efficiency).

The data economy represents a significant global economic, political and social opportunity, however the enabling regulatory environment plays a critical role in ensuring how well this opportunity is leveraged for Australia's economic growth and citizen experience.

We forecast that it will be the markets who establish themselves as 'leading light' progressive data policy-makers who will benefit the most from the open data opportunity. These markets will be best positioned to harmonise their open data governance model and infrastructure, capturing a disproportionate share of global data flows, as well as owning higher value activities along the data value chain (e.g. job creation in the increasingly lucrative fields of analytics, data engineering, data scientist and cryptography).

Australia is well-positioned to disproportionately gain from this emerging data economy by virtue of its:

- Highly digitised developed economy (which is rich in data as a natural resource)
- Relatively concentrated market structure (which can be harnessed for at-scale execution and cross industry collaboration more easily)
- Relatively mature and sophisticated data market (Government Open Data, corporate adoption of data sharing, Open Banking, Consumer Data Right etc)
- Considered approach to data policy development (albeit fragmented and unaligned to a cohesive macro strategy) and relatively balanced perspective on privacy versus innovation
- Commitment to consumer and citizen empowerment in the broader digital and data economy (Consumer Data Right and Digital Platforms Inquiry outcomes)

The Australian Government's Consumer Data Right (CDR) is an example of progressive data legislation which sits ahead of this curve, delivering greater controls for consumers to direct or protect data as they see fit. However, in our view the current CDR reforms do not go far enough to allow Australia to reap the productivity and innovation benefits of the global data economy opportunity.

### Limiting factors include:

- The CDR is banking and fintech centric - Current legislation has been designed to enable Open Banking first but the current systems designs are too narrow. There is the risk that the proposed data portability mechanisms will struggle to scale/be relevant across all industry verticals.

- An unsophisticated approach to consent. Consent and consent management is a fundamentally important infrastructure layer in the data economy in its own right. The full portent of an encoded consent model ubiquitously adopted through an open source protocol is not considered in the current design.
- The creation of systemic risk in Australia's data ecosystem by designing and architecture data flows to replicate citizen data records and create more and more 'data honey-pots' across the economy.
- A lack of recognition on the true scope of Australia's data economy. CDR has to date only focussed on consumer directed "pull" use cases (*a competitor pulling on incumbent data against their wishes*) and largely ignored enterprise directed "push" use cases (*one enterprise/organisation voluntarily sharing data with another with consumer consent*). The scope for B2B or peer-to-peer "push" use cases to improve Australian economic productivity and innovation is being largely ignored.
- A lack of harmonisation with emerging international data portability standards - limiting our potential when it comes to future cross-border data trades and exporting Australian technology capability.

For Australia to reap the benefits of the emerging global data economy, the Consumer Data Right must be expanded to be able to practically function across all industries, adequately address the findings of the Digital Platforms enquiry when it comes to consumer choice and consent and lay down the foundations for Australia's future cross-border trade in data.

The pages below outline our recommendations to make this possible.

## 1. Consent Management: The critical layer we need to get right

The data economy is broad and complex with many layers that need to interoperate in order to function.

Data, unlike money, has an almost infinite capacity for value or insight creation. It can be used, manipulated, combined and re-used. Globally, data ecosystems are being developed to allow for many specialist capability providers to deliver services and many different strategies to be adopted by participants, maximising the potential for innovation.

These many layers exist in varying capacities across the Australian data economy today. Every day millions of Australians generate terabytes of data. All of this data requires interaction with different constituents in our data economy from the individual consumer to advertising platforms, to enterprises, to startups and scaleups building applications or data science teams working on health or government policy. These ecosystem layers grew organically and as the Digital Platforms Inquiry (among various other Australian government initiatives) has revealed, there has been a clear power imbalance for some time. The Australian Consumer Data Right is a major, innovative policy lever which seeks to address data control, privacy and liquidity issues in our current system and empower consumers.

However - the most important enablement layer which underpins data economy participant ability to move data with trust, **Consent Management**, has been considerably underdeveloped in the current legislation/policy framework.

Under the current CDR legislation, consent is treated like a static precursor to the act of the data movement itself. The Consumer Data Right currently provides for 'read' access, that is, the transfer of data about a customer to them or a trusted third party at the customer's direction and with their consent. A consumer cannot give consent to 'write' or modify data on their behalf, limiting the utility of their data when it comes to switching activities.

And the current [Consumer Experience Standards](#) only clearly proscribe Data Language Standards associated with Open Banking use cases. Under the current approach, providing consent for 'read' access is likely to prove complicated and confusing for consumers if metadata labels (or Data Language Standards) will be defined differently between industries.

Effective Consent Management requires that consent become a critical infrastructure layer in the system and be built in a way to incentivise a ubiquitous adopted, consumer centric protocol. It should be simple, unbundled and granular, and systemically ingrained - giving opportunity for consumers to have full control and determine how much data to share, with who and for what purpose; equally to give data collectors ability to tailor products, services and incentives to match consent (i.e. if a consumer has a narrow consent then they just get the service with no frills, if they have a broad consent then they get the service with frills (could be loyalty points, a discount, special offers)).

In our view, the concept of consent in CDR must evolve from a relatively simple workflow and UX recommendation with no standardised approach to use case taxonomy to a highly standardised, software enabled, taxonomical consent model which encodes consent and enables it to flow through a system capturing critical information at a use case level.

The fundamental elements of Consent Management are:

- **That the consent is expressed** - that is that the consumer makes an active choice to consent, rather than is taken to consent by implication or silence.
- **That the consent is unbundled** - that the consent for data sharing, if broader than absolutely necessary to deliver the product or service, is not a condition of receiving or obtaining that product or service. The customer should have the ability to determine how broad or narrow the consent is.
- **That the consent is simple** - that the scope of the consent is easy to consume and understand and is built upon a standardised taxonomy. This is primarily a Customer Experience requirement and will drive consumer education through repetition of experience. Once consent is standardised it is then capable of being encoded.
- **That the consent is revocable** - that the customer has the ability to withdraw the consent at any time.
- **That the consent is time-bound** - that the consent is not indefinite or not effectively indefinite (for example an excessively long time-period). 12 months is often tossed around as an absolute limit.
- **That consent be assignable** - so consumers have the ability to assign granting of consent to a specialist, trusted consent advisor. In the event of a successful, highly liquid data economy, this would be necessary to address “consent fatigue”.

Critically, in order to provide an empowering, educating experience for consumers and a valuable, practical implementation for consumer facing organisations, the elements of Consent Management set out above need to be capable of codification and a common taxonomy of permitted uses developed. This takes the existing Consumer Data Right framework further into a more practical, easily adoptable framework.

**We strongly advocate for the creation of an open source *Consent Management Protocol* built on a standardised taxonomy of use cases to enable both the codification and implementation of dynamic consumer consent at an API level.**

It's clear that a properly constituted dynamic approach to consent capture, codification and management (A Consent Management Protocol) would help the CDR regime overcome the technical and experiential difficulties associated with rolling out the regime across multiple industries. Parallel industry groups could be created to agree upon the relevant taxonomy which could be implemented utilising a consistent technical protocol.

Our view is that a properly constituted Consent Management protocol/ layer would effectively solve for the following issues in the current CDR legislation/ policy approach:

- Allow for the ready of expansion of CDR to all industry verticals (by virtue of a common consent protocol).
- Solve for the unbundled consent recommendation from the ACCC Digital Platforms enquiry.
- Address a portion of the consumer education requirement under CDR through repetition of experience (training consumers on what good, consent based data sharing looks like).
- Enable a private sector collaboration on a codified consent taxonomy while preserving a role for regulators to endorse (more market centric and rapid development).
- More readily enable B2B/ Peer-to-peer ‘push’ data sharing use cases in addition to pull (voluntary adoption by industry).
- Transform consent into code which makes it systematically useful and could enable a data regulatory monitoring framework (meta data from the common protocol could be made available to the regulator to monitor activity in the data economy).
- Future-proof Australia’s position in the global data economy by becoming a central protocol/ standard for international data cooperation (which could then underpin cross-border trade in data)

**Most importantly, in a practical sense, this approach would enable consumers to manage their consents through a centralised consent wallet, according to the level of granularity they desire.**

The above recommendations are backed-up by recent findings from primary market research conducted by Data Republic in 2019 to define consent management use cases, jurisdictional considerations, constraints and commonalities, as well as enterprise perspectives on current consent management models.

This research involved interviews with existing Data Republic and clients, industry leaders and governments who are at the forefront of both the evolution of consumer consent laws and their required enactment in business. As well as consumer focus groups across different regions to better understand variance of consumer understanding and sentiment towards consent models and the role a consent management system could play in empowering and shaping future consumer sentiment.

#### **Activity Overview:**

- 2 Continents & Regulatory Jurisdictions
- 5 Industries, 10 companies, 2 consumer focus groups

#### **Key Findings:**

- *Consumer Hypothesis confirmed:* Consumers prefer Consent flows that are explicit, unbundled, revocable, simple and time-bound compared to traditional static T&Cs and privacy policies. A consistent message that emerged from this was that consumers found a simple consent model to be an “awakening” with regard to their understanding of data sharing and confidence in doing so.
- *Consumer Hypothesis confirmed:* Consumers are more willing to invest in understanding and granting consent when it is presented in a granular and consistent way across industry use cases.
- Enterprises in Australia and Singapore have similar data sharing concerns and Consent Management is emerging as a priority in C-suite strategy.
- When interviewed on their capability to technically comply with the principles of fine grained consent (*express, unbundled, simple, revocable, time-bound*) all of the companies indicated a lack of preparedness and the requirement for significant investment and planning.
- When interviewed both enterprises (and some regulators) in Singapore and Australia said they would prefer an ecosystem wide, open protocol for Consent Management that would facilitate and maximise collaboration across enterprise and geographies.
- All enterprises interviewed acknowledged that a common, interoperable Consent Management protocol/layer would enable new opportunities for businesses to create both enterprise and consumer value. Use cases were ranked according to anticipated value creation and a variety of B2B/ peer-to-peer data sharing use cases were uncovered signalling potential economies of scale/innovation and productivity benefits.

*Please see the [appendix](#) for further information on our recent consent management market research.*

It is our view, confirmed by both our recent market research and frontline experience of 4+ years delivering software and technologies to enable safe, privacy-preserving data



collaboration, that an open source Consent Management protocol would serve the major strategic objectives of the CDR. It would empower and give control back to consumers while enabling greater data liquidity and utility (through consent surety) across the various participant layers in Australia's data economy.

The alternative is a slow trudge rolling out CDR from one sector to the next, with a very real risk of lack of interoperability across industries, confused consumers failing to adopt and years of implementation before Australia can reap the economic, productivity and innovation benefits of controlled data liquidity. By then, of course, Australia will have missed the opportunity to become a leading-light in the global digital & data economies.

#### **Recommendation:**

- The Data Standards body in consultation with industry and consumer groups should develop a consent taxonomy standard which codifies permitted use cases and known consent variables, dimensions and triggers.
- This taxonomy should be used to develop an open source *Consent Management Protocol* to enable both the codification and implementation of dynamic consumer consent at an API level.

## **2. Expanding access: A controlled CDR-utility layer for SMEs/startups**

In addition to designing and implementing an economy-wide taxonomy for Consent Management, we believe there is also an opportunity for the Australian government to expand access for innovative startups and SMEs to Consumer Data Right by re-thinking raw data portability as the sole data flow channel for accredited parties.

The current standard design of Consumer Data Right relies on the replication and free-flow of raw banking and transaction data from one entity to another, generally from a higher security environment to a lower one. We believe that this architecture has the potential to create systemic risk to the nation's data economy by proliferating citizen data honeypots and placing undue compliance burdens on startups and FinTechs who by their very nature need agility and support to grow.

Instead of mandating raw customer data to flow from high-security environments to be replicated in FinTech environments, we recommend developing an alternative CDR data operating channel whereby the current 'Data-to-Algorithm' model (moving raw data to processor capability) could be complimented by an 'Algorithm-to-Data' model (moving the data processing capability to the raw data).

#### **The basic principles of the Algorithm-to-Data approach are:**

- Raw data is not transferred directly to a FinTech/recipient, or is only transferred temporarily to a secure space (from which it cannot be extracted in its raw form) and held temporarily until processing is complete then deleted.
- Value is created out of data by applying algorithms (that belong to the Fintech/startup) to the data to generate an approved output for the recipient. For example a confirmed credit reference check.
- The output may be extracted and transferred freely with the consent of the customer.
- The original custodian of the raw data set retains control over the raw data set and is able to allow the customer to exercise their rights without having to transfer control of the raw data set to the new Data Processor/recipient.

It's helpful to consider an analogy to airports and customs here where “diplomatic zones” for data could be created to enable raw data from one organisation to be temporarily landed to enable a joined data product to be created and “moved through customs” (governed flow into recipient organisation) while the raw data was “deported” (deleted).

A cost effective opportunity for FinTechs/CDR Data Recipients would be a co-funded utility from government and industry which could provide an intermediary orchestration layer. The utility would have the security necessary to hold raw data and would deal with that data on behalf of the CDR Data Recipients. CDR Data Recipients would provide their algorithm to the utility who would apply it to the data. Data Recipients would pay a nominal fee to access the utility (either per-use or annuity). This would mean that a Data Recipient would no longer need to invest the same level of resources/times into security and accreditation thresholds in order to leverage the CDR opportunity.

#### **Recommendation:**

- Co-fund a CDR utility layer between government and industry to provide a secure intermediary and orchestration layer for emerging startups/FinTechs & SMEs to access the CDR regime and boost Australian innovation, economic outcomes without undue compliance burdens.

### **3. International developments & harmonisation - Future Proofing Australia's Consumer Data Right**

As the CDR Issues Paper rightly outlined, we are at a regulatory and technology inflection point:

- Data sharing and privacy laws are top of mind for many regulators across the globe. There have been huge data policy shifts across the UK, EU, APAC and USA over the past five years.
- Data sovereignty/localisation is emerging as a key theme which will need to be considered in any data policy framework.
- As regulatory frameworks mature, consent is evolving from traditional binary models of a ‘yes/no’ captured at a single point in time to a multifaceted concept, contemplating various levels of granularity.
- There is a clear need for the creation of “rails” for the movement of data products and consent across jurisdictions.
- A significant opportunity exists for early-movers to shape the standards for global Consumer Consent Management approaches.

If the 19th century was the age of industrialization and the 20th century the age of commercialisation, the 21st century is shaping up as the age of data-driven expansion. High functioning data ecosystems have become critical to sustaining economic growth. As such, resolving the inconsistencies between various jurisdictions' data regulations will be a key feature of future trade negotiations. It is also likely to form an increasingly well-delineated part of national economic identities that are being reshaped by countries' participation in emerging data-driven economies.

We have observed in the emerging domain of data, and in particular the regulation of data, a significant early-mover advantage for nations when it comes to data policy development and

implementation. The EU implementation of GDPR is often talked about as the global standard for data protection and is the inspiration for the CCPA in California. In addition, the UK Open Banking Model has been well marketed as the standard for Open Banking globally. It is clear that GDPR and UK Open Banking have both been hugely successful national branding exercises in data policy. They have demonstrated the importance of moving quickly in response to shifting global sentiment and technology innovation.

In recent years, there has been a global emergence of data portability and protection schemes:

- Regulated Open Banking and/ or Open data/portability systems have been established in the European Union, the United Kingdom and Australia and one is being considered in Canada.
- Voluntary frameworks are being established or considered in Singapore, India, Japan, Hong Kong, South Korea, Malaysia, Indonesia and New Zealand.
- General rights to portability of personal information exist under the data protection, or privacy, laws of many jurisdictions including the European Union, Australia, Singapore, Hong Kong and California.
- Commercial arrangements have arisen in China and the United States through a combination of bilateral commercial arrangements, without any regulatory coordination.

The race to lead the world's data economy has accelerated recently with the Feb 2020 launch of the European Commission's Data Strategy which addresses their own GDPR 'innovation obstacles' in favour of standardising and scaling governed data flows.

**Relevant excerpts include;**

*"The EU should create an **attractive policy environment** so that, by 2030, **the EU's share of the data economy** – data stored, processed and put to valuable use in Europe - at least **corresponds to its economic weight**, not by fiat but by choice." (p4)*

*Those tools and means include **consent management tools**, personal information management apps, including fully decentralised solutions building on blockchain, as well as personal data cooperatives **or trusts acting as novel neutral intermediaries in the personal data economy**. Currently such tools are still in their infancy, although they have significant potential and **need a supportive environment**. (p10)*

*This could include a mechanism to prioritise standardisation activities and to work towards a more harmonised description and overview of datasets, data objects and identifiers to **foster data interoperability (i.e. their usability at a technical level) between sectors and, where relevant, within sectors**. (p12)*

*Concretely, the Commission intends to fund the establishment of **EU-wide common, interoperable data spaces** in strategic sectors. (p16) The spaces will include: (i) the deployment of data-sharing tools and platforms; (ii) the creation of data governance frameworks; (iii) improving the availability, quality and interoperability of data – both in domain-specific settings and across sectors. (p17)*

*The EU should take advantage of its effective data regulatory and policy framework **to attract the storage and processing of data from other countries and regions**, and to **increase the high value-added innovation** that arises from these data spaces. Companies from around the world will be welcome to avail of the European data space, subject to compliance with applicable standards, including those developed relative to data sharing. (p24)*

**The Australian Consumer Data Right, announced in 2017, was a world-leading data policy initiative but it has been slow and narrow in implementation and now risks losing its global relevance.**

The core opportunities we see for Australia in a revised CDR are as follows:

- a) Implement the proposed changes outlined above (*Consent Management protocol, CDR utility layer*) to provide a highly functional cross-industry Consumer Data Right model.
- b) Seek opportunities to collaborate with like-minded markets on a common approach to an open source Consent Management standard (UK, Singapore, EU etc).
- c) Develop technical and policy approaches to facilitate functional cross-border data trade in a way that recognises and is compatible with emerging data sovereignty and regulatory trends from other progressive data economies (UK, Singapore, EU).

Expanding Australia's foreign data policy approaches under a revised or expanded Consumer Data Right legislation should take into the consideration the following:

**(1) The development of common foundational definitions for cross-border data-sharing**

- a. There is a need to harmonise on certain critical definitions and ideally taxonomies and to create space for those concepts with regard to the relevant domestic laws. This is particularly the case where data sovereignty (the retention of PI and other relevant data relating to citizens within that jurisdiction) continues to be a regulatory trend.
- b. For instance, under future data Free Trade Agreements recognition, where that PI which has undergone a technically rigorous process of tokenisation and sharding (breaking the hashed result into small fragments prior to leaving the jurisdictions domain) is not PI for the purposes of the Australian Privacy Act and does not breach the concept of data sovereignty where it occurs through an approved channel would be critical to enabling cross-border data sharing.
- c. Ideally, there would be space created to allow industry to harmonise on common taxonomies, permitted uses, simple consent definitions etc which would permit data products to move across borders with greater ease/less friction. This is not essential to the minimal functioning of a data Free Trade Agreement but would materially improve liquidity across markets over time. This could be completed on an Industry by Industry basis.
- d. Further questions to be considered for cross-border data policy harmonisation could include:
  - o What constitutes raw data?
  - o What constitutes personal data?
  - o What constitutes a data product / value added data?
  - o Categories of permitted uses for certain types of data?
  - o Consumer consent taxonomies

**(2) Approved data trade channels and regulatory oversight**

- a. We envisage a process where cross-border trade in data is done through approved channels so that licensing of data and data products (insights, algorithms, applications) can be tracked, monitored and reported to create a transparent regulatory system.
- b. These approved channels should be able to differentiate between raw data and a derivative data product/algorithm/application. We should encourage the flow of data products through approved trade channels while leaving PI and raw data in sovereign countries (to

the best extent possible). Alternatively, where raw data is permitted to flow, there is at least an auditable record of it.

- c. Regulatory oversight of licenses – it should be possible to incorporate a regulatory body into a licensing process to provide pre-approval for a proposed cross-border data movement or transaction under consideration (i.e. DBS and WBC “agree” and both IMDA and ACCC “approve”) or provide a reporting mechanism to log and surface all cross-border data shares if no pre-approval was needed.
- d. These approved channels could enable concepts such as “international waters” for sharded PI matching and “diplomatic zones” for data temporally landed to enable a joined data product. Which could, in turn, be part of the regulatory tracking process above. It would even be possible to enable approved, persistent Diplomatic Zones between countries so that permanent flow of de-identified data can occur (i.e. tracked, reported, approved, etc). A kind of “cooperative data warehouse/workspace”.
- e. These channels would also enable regulatory and taxation approaches to be streamlined to support the export of Data Product IP between countries (algorithm-to-data), for example; Analytical models, credit models, AI/ML applications, data applications.

### **(3) Recognition of PI sovereignty**

- a. Our recommendation is that even if Australia is comfortable with the idea of raw data flows between ‘accredited’ nations, best attempts should be made to design a framework that honours emerging data sovereignty policy trends wherever possible, as like GDPR, this will emerge as the most difficult standard to navigate.

### **(4) Collaboration on specific technology/policy interplays**

- a. New technological capabilities can be developed which will facilitate the potential for approved cross-border trade in data.
- b. An open sourced Consent Management protocol developed in conjunction with other jurisdictions could be a critical enabler for regulated cross border trade in data.
- c. It is possible to then leverage that capability into a data Free Trade Agreement to facilitate a higher functioning version of cross-border data sharing.

### **(5) Recognition and adoption of common infrastructure, technology principles**

- a. Similar to the Consent Management protocol above, technology infrastructure such as Data Republic’s decentralised, privacy-preserving matching network could be recognised as approved common infrastructure under a data Free Trade Agreement.
- b. Such an approach would allow for greater regulatory oversight as to data-sharing activity and trade occurring on that infrastructure as well as giving greater confidence to enterprises and government organisations interested in conducting cross-border data sharing in the near term.

By demonstrating an effective model for both *intra*-national data portability/movement as well *inter*-national / cross border data trade, Australia would be well placed to provide an effective example for other data economies to follow.

The regulatory mirroring, likely to follow, would allow Australia to capitalise on early development of a global data economy, as well as the economic and productivity gains which come from owning higher value activities along the data value chain (e.g. job creation in the increasingly lucrative fields of analytics, data engineering, data scientist and cryptography).

**Recommendation:**

- Ensure CDR technical standards continue to be interoperable with UK, Singapore and EU standards (API).
- Develop a common approach to Consent Management with like-minded jurisdictions with a view to enabling data sovereignty honouring cross-border regulated trade in data.
- Support “policy proto-typing” exercises between governments, industry partners and consumers to explore cross-border data trade use cases and required legislative amendments.
- Ensure that any proposed cross-border policy framework can be tested in parallel with a practical Proof of Concept. The outcomes from this technology enabled approach can help inform a final Australian data policy position on potential Data Free Trade Agreements.

### 3. Drive efficiency and productivity through a centralised Data Agency

The Consumer Data Right has established solutions to problems that may also exist elsewhere in the digital economy – in particular, in relation to data sharing, data portability and custodianship of data.

Data Republic agrees with the CDR Issues Paper assertion that *“There are a range of existing regulatory frameworks that seek to address similar problems – often in potentially inconsistent or industry-specific ways which are not compatible or interoperable with each other.”*

Australia has a rapidly evolving and sophisticated approach to policy development with regard to data, including:

- Consumer Data Right – a fundamental and foundational principle which underpins the increased liquidity of data and is a key enabler of a data economy;
- Open Banking – the first practical implementation of a Consumer Data Right (CDR) to an industry vertical. It seeks to address core issues including authentication, security, technical standards and data standards and is framed as a model for application to future industry verticals;
- Data sovereignty – Australian Prudential Regulation Authority (APRA) has additional oversight of data being stored offshore
- Open government data – Productivity Commission recommendations of formalising an approach to opening up of government data under proposed Data Availability and Transparency Bill to be passed in June 2020. The National Data Commissioner role was established to oversee this.
- Digital ID – Digital Transformation Agency (DTA)-driven framework for federated digital identity models which have the potential to be adopted across both the public and private sectors. Draft legislation addressing liability limitations of Digital ID for KYC also lay down the framework for a more liquid and efficient data economy. Digital ID is one of the foundational capabilities for it.
- ACCC Digital Platform Unit & Code of Conduct - Recently announced by the government to monitor and report on the state of competition and consumer protection in digital platform markets.
- ACCC Digital Platform proposed changes to Australian Privacy Law - Driving greater alignment with GDPR by imposing higher consent thresholds and introducing rights to deletion.
- DFAT are leading discussion between nations (such as Singapore and Australia) on Digital Economy Agreements (aka a Digital Free Trade Pact) to drive 'greater connectivity' and bilateral economic relations, with cooperation touted to encompass several areas including e-payments, fintech, artificial intelligence (AI), and digital identity.
- Privacy Act refresh - under the jurisdiction of the OIAC and the Attorney General's office.

However, Australia's regulatory framework for data is largely piecemeal and lacks coordination, potentially creating suboptimal implementations of many of these initiatives. There is no clear accountability for either the constructive development of a domestic data economy (accelerator) or holistic regulation (brake) of a domestic data economy.

In order to be a global leader, Australia should undertake a process of regulatory centralisation with respect to the Data Economy. Currently, regulatory responsibility for all relevant elements

of the data economy are split across multiple different bodies or government departments, including:

- Australian Securities and Investment Commission (ASIC) – appears to hold responsibility for regulatory sandbox initiatives and cross border regulatory harmonisation relating to data.
- APRA – has regulations relating to financial services data (sovereignty, utilisation of cloud technology, presence of data outside of firewall etc). APRA also holds oversight on financial services problems which are ostensibly data sharing problems (income verification, expense verification, responsible lending, CCR etc);
- Australian Competition and Consumer Commission (ACCC) – newly-introduced agency with responsibility for oversight and enforcement of the Consumer Data Right and Open Banking regulation, as well as driving outcomes from Digital Platforms Inquiry;
- Data61 appointed Data Standards Body with responsibility for the technical implementation of the CDR regime across banking, energy, telco;
- Austrac – data driven policing of KYC and AML (both of which are data sharing and digital identity problems);
- DTA – under Department of Prime Minister & Cabinet, holds the policy framework for the National Data Commission, Digital identity and federal Open Data strategy;
- Office of the Australian Information Commissioner (OAIC) – responsible for privacy regulation and enforcement of APP's;
- Home Affairs – responsible for cyber-security, which is inextricably linked to the design, development and regulation of a data economy.

At Data Republic, we've witnessed the consequences of this fragmentation in the following ways:

- Confusion within and outside of government about departmental ownership and mandate for different components of the data value chain. Therefore, we've experienced no clear pathway to engage with the government as either a vendor or a policy advisor (Data Republic is actively working in global markets in a manner facilitated by central government agencies).
- Piecemeal legislation and policy action ignores the fact that data is a by-product of systems and requires a systems-based approach to both opportunity and risk management. Solving one data policy issue at a time with disparate departmental leadership has created a labyrinth of competing data priorities and compliance burdens, e.g. Open Banking, Austrac AML for banking. Therefore, significantly reducing private sector bandwidth for value creation with data. Data has become a one-sided risk conversation to the detriment of our national productivity.
- Government competition with private enterprise: The role of the CSIRO and more specifically Data61 appears to be at odds with the Government's mandate of competitive neutrality. We often find Data61 competing directly with private enterprise for government and non-government work. This is further complicated by the quasi-regulatory role that Data61 plays as the CDR Data Standards Body.

By consistently taking a narrow-view, for example just focusing on Open Banking and FinTech - we ignore the fact that the majority of the issues arising from the Digital Platforms Inquiry, Banking Royal Commission and Productivity Commission in large part can be traced back to a lack of design and proactive regulation of Australia's data economy.

The ACCC have done an admirable job to move so rapidly up the data learning curve but the data economy opportunity for Australia is much larger than simply a competition or consumer issue.



## A contrasted approach – Singapore’s IMDA

Both this policy development and regulatory fragmentation should be contrasted with a model like Singapore’s which has evolved rapidly to a single executive branch for the data economy which has a paired model of accelerator (innovation, industry development) and brake (privacy, sovereignty etc).

The IMDA is a statutory board in the Singapore government, that seeks to deepen regulatory capabilities for a converged info-communications media sector (i.e. data) while safeguarding the interests of consumers and fostering pro-enterprise regulations. Its vision is to create a “Vibrant, World-class Info-Communications Media Sector that Drives the Economy, Bonds Communities and Powers a Smart Nation”. It is chaired by the Permanent Secretary of the Ministry for Defence, which demonstrates the strong linkages between cybersecurity and a data economy.

Within the IMDA, the paired brake/accelerator model reports under a single statutory authority (separate sub-branches) which allow for nuanced decisions to be made that might require consideration of trade-offs between privacy and innovation. These two sub-branches are:

- Personal Data Protection Commission – whose mission is to “promote and enforce personal data protection so as to foster an environment of trust among businesses and consumers, contributing to a vibrant Singapore economy”;
- Data Innovation Programme Office (DIPO) – stated ambitions include facilitating data-driven innovation projects, and the development of Singapore’s data ecosystem. DIPO will introduce a Data Sandbox Programme, a trusted platform for companies to share data across sectors.

These capabilities have been organised to deliver on Singapore’s stated ambition “to build the world’s first “global data exchange”, based in Singapore”. Given a coordinated and comprehensive top down data strategy, the ability to organise industry and Singapore’s status as a progressive yet privacy-centric country, they are well-placed to achieve this vision.

### Recommendation:

- Streamline Australian data economy regulation and industry development under one dedicated government body to allow for greater transparency, accountability and effective engagement with private industry. We need to bring together all the different arms of data policy under a core regulatory body that creates a new industry and regulates it.
- Ensure that Data61 not be able to continue the current practice of ‘gamekeeper’ (advising on policy development with privileged access to government) and ‘poacher’ (developing practical technological solutions within those same domains in competition to the private sector).

## 4. Consumer Protection

Data Republic is supportive of the comprehensive approach being taken by the ACCC and Data Standards Body when it comes to consumer protection under CDR.

It is our view, supported by our recent consumer focus group findings (*summarised on appendix page 23*) that the most effective way to ensure consumer protection, transparency and control as CDR develops is to:

- Adopt the data-economy wide open, interoperable Consent Management model outlined above.
- Utilise the consent taxonomy embedded in the Consent Management protocol to underpin simple, intuitive consent management user interfaces for consumers - enabling "education through repetition".
- Leverage interoperable Consent Management technical systems to provide a unified regulatory monitoring system which protects consumer rights.
- Support the growth of an additional participant layer in Australia's data economy - outsourced Consent Management or the creation of "Data Asset Managers" for consumers whereby organisations can engage directly with consumers through that consent wallet or through the use of agents acting on their behalf to ensure each consumer is getting the maximum benefit, utility and value from their data. (Accreditation would be required under CDR).

### Recommendation:

- Develop and embed a data-economy wide Consent Management model that empowers consumers to participate in CDR.

## About Data Republic

- Data Republic is an early stage, home-grown Australian technology company with global ambitions. We have offices in Sydney, Singapore and Los Angeles.
- Our leading technology enables organisations to govern data movements and licensing through a private-by-design platform, transforming manual governance procedures and patched-together analytics solutions into simple, online workflows. Importantly, Data Republic's patent-pending privacy-preservation technology enables organisations to match datasets across organisations (and borders) without exposing raw personal information.
- Data Republic was founded in Australia in 2015 and raised Series A investment from tier one Australian corporates including Westpac Banking Corporation, National Australia Bank, QANTAS, with ANZ Bank also investing in a Series AA round.
- In December 2018, Data Republic completed a further capital raise (Series B) with follow-on investments from WBC and ANZ, as well as new investment from tier one Singapore corporates, Singtel and Singapore Airlines and Singapore based VC, Qualgro.
- The presence of these established Singaporean and Australian corporate giants on the capital table of a start-up like Data Republic is evidence of the shared challenges to which Data Republic is a solution. The governed, secure, auditable and privacy compliant exchange (or sharing) of data between organisations.

## Concluding Note

Data Republic is open to continuing exploratory discussions on the above-outlined recommendations.

We thank the Australian Treasury for the opportunity to make a submission to this Inquiry.

Please direct any follow-up questions or queries to [danny@datarepublic.com](mailto:danny@datarepublic.com).

Kind Regards,



**Danny Gilligan,**  
CoFounder & CEO, Data Republic

## APPENDIX:

### Insights from Data Republic Market Research into Consent Management Models

Across 2019, Data Republic conducted market research to define consent management use cases, jurisdictional considerations, constraints and commonalities, as well as enterprise market interest in comprehensive consent models which could inform future Data Republic product design.

This research involved interviews with existing Data Republic and clients, industry leaders and governments who are at the forefront of both the evolution of consumer consent laws and their required enactment in business. As well as consumer focus groups across different regions to better understand variance of consumer understanding and sentiment towards consent models and the role a consent management system could play in empowering and shaping future consumer sentiment.

#### Activity Overview:



- 2 Continents & Regulatory Jurisdictions
- 5 Industries, 10 companies, 2 consumer focus groups

#### The interviews:

As part of this project, Visa and Data Republic interviewed a total of ten companies across five industries in Australia and Singapore.

#### Industries:

These companies interviewed were all multinationals and industry leaders in their respective verticals, and the meetings were attended by people at the highest levels of the organisations across multiple parts of the business, as seen in the exhibit below.

	Banking/Insurance	Telco	Airline	Government
 AUSTRALIA	✓	✓	✓	✓
 SINGAPORE	✓	✓	✓	✓

On the following pages we've summarised some of our findings most relevant to the Inquiry into Future Directions for the Consumer Data Right.

## a) Towards a Consent Taxonomy

A key focus of the market research was to explore whether the development of a common CDR consent taxonomy could allow consumer consent to be codified and permitted use cases made portable across multiple use cases and industries.

In order to have universal consent that can be codified and portable across enterprises and borders, it needs to be captured in a way that is consistent across multiple use cases and regions. To inform our understanding of consent across data-sharing use cases, workshops were held to identify the key dimensions of each common consumer use case for data portability under an open data regime like Australia’s CDR.

We developed the below indicative **Consent Taxonomy framework** which allows each consent capture to be broken down into different parts, some fixed and some variable, that can then be standardised or codified across an industry or data economy.

This framework and the below example use cases were then tested through interviews with participating enterprises. Multiple sources of guidance on consent were combined, rationalised, and tested, including:

- Existing consumer consent-flow structures in the market
- Customer experience best practices from trusted brands
- Anticipated future consent regulation
- Extensive consumer research and focus groups

### Data Republic - Consent Taxonomy Framework

Use case definition	Drivers	Key elements of Consent	
<p><b>Components</b> <i>The different items making up a use case</i></p> <ul style="list-style-type: none"> <li>• Data holder</li> <li>• Data field(s)</li> <li>• Purpose</li> <li>• Duration</li> <li>• Frequency</li> <li>• Data receiver/ third party</li> </ul>	<p><b>Underlying drivers</b> <i>The primary reason why Consent is captured</i></p> <ul style="list-style-type: none"> <li>• Regulation</li> <li>• Customer need</li> <li>• Competition/ market</li> <li>• Corporate policy/ procedure</li> <li>• Other</li> </ul>	<p><b>Granular elements</b> <i>The way that Consent is captured</i></p> <ul style="list-style-type: none"> <li>• Express/explicit</li> <li>• Unbundled</li> <li>• Revocable</li> <li>• Simple</li> <li>• Time-bound</li> </ul>	<p><b>Capture/sharing methods</b> <i>The foundational approach to capturing Consent/sharing data</i></p> <ul style="list-style-type: none"> <li>• Opt-in</li> <li>• Opt-out</li> <li>• Push to 3<sup>rd</sup> party</li> <li>• Pull from 3<sup>rd</sup> party</li> <li>• Read Access</li> <li>• Write Access</li> </ul>
<p>Underlying drivers, granular elements, and capture/sharing methods will vary depending on data holder, geography, and other factors specific to the use case</p>			

Examples of the consent taxonomy components can be found below.

### Use-Case Components

	Data Holder	Data Field(s)	Purpose	Duration	Frequency	Data Receiver/ Third Party
Definition	The entity that holds the specific data	The specific data required in the use case	The reason data is shared	Length of time that consent is granted	How often data is accessed	The third party that will receive the data in the use case
Examples	Bank Telco company	Transaction data Income data Location data	To receive personalized offers	One-time Specific period Indefinite	Realtime Context based Periodic	Merchants Government Marketing firm

### Underlying Drivers

	Regulation	Customer Need	Competition/ Market	Corporate Policy/ Procedure
Definition	Regulatory forces influences the capture of Consent	The customer requests or demands that their Consent is captured	Consent is captured to gain a competitive edge, in response to competitor actions, or to unlock new revenue opportunity	Capturing Consent is part of corporate policy or procedure (and NOT driven by regulatory constraints)
Example	GDPR requires company to capture Consent	Customer demands you obtain Consent when selling their data	Boost brand by capturing Consent or Consent grants access to new data that opens revenue opportunities	Company decides that capturing opt-in Consent should be normal procedure

### Granular Elements

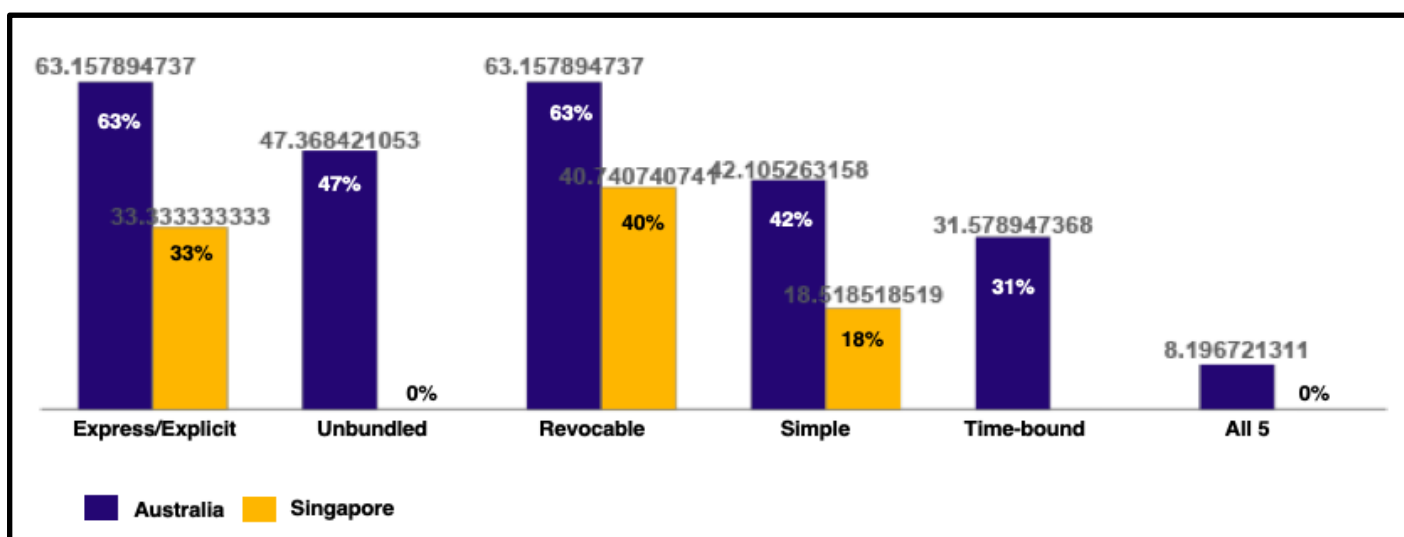
	Express/Explicit	Unbundled	Revocable	Simple	Time-Bound
Definition	Consent is given specifically rather than implied by customer actions	Consent is specific to the use case and not bundled with other use cases	Consent can be revoked at any time	The terms of the data-sharing use case are clear and easy to understand	Consent is for a defined period of time, after which new Consent must be obtained
Example	Customer gives Consent in writing	When a customer gives Consent, they give Consent for one use case; Consent is not bundled in T&Cs	Customer can unsubscribe from marketing communications at any time	Notice clearly states what data will be shared, with whom, what it will be used for, and how long	Customer Consent expires after one year and must be renewed

### Capture/ Sharing Methods

	Opt-In	Opt-Out	Push Data to 3 <sup>rd</sup> Party	Pull Data from 3 <sup>rd</sup> Party	Read Access	Write Access
Definition	The customer will have to explicitly opt-in for the use case	By default, the customer gives Consent and must opt-out to revoke	Data will have to be pushed to a third party in the use case	Data will have to be pulled from a third party in the use case	The ability to read the data	The ability to manipulate the data
Example	Explicitly clicking a button or checking a box	Customer data is included in an aggregate unless they opt-out	Bank pushes data when a consumer makes a purchase in Uber Offers	Bank pulls airline miles data into a single view portal	A credit provider checks consumer's credit score	Marketing firm analyzes transaction data to target consumers with ads

### Key findings from market research testing on Consent Taxonomy:

1. Codifying different consent elements into a common taxonomy or framework does assist businesses to better understand data sharing use case requirements and how to evaluate and support interoperability across business units and jurisdictions.
2. When evaluated against the principles of fine grained consent (express, unbundled, simple, revocable, time-bound) it is **clear that clients are unprepared for future dynamic consent management regulations**. See below proportion of currently executable B2B data-sharing use cases that would meet each granular consent requirement, by country.



3. There is a clear need for interoperable consent management tooling and guidance for enterprises on how to support dynamic consumer consent under emerging regulations like CDR or Singapore's Data Portability Act.

### b) Consumer attitudes

In addition to exploring enterprise readiness for emerging consent management models, we also hosted consumer focus groups in Singapore and Australia to test consumer attitudes about consent management and control of personal data flows.

Each group was a different mix of ages, levels of comfort in sharing data, and approaches to privacy protection.

Group One	Group Two	Group Three
<b>High Awareness/Active Protection – all ages</b>  •Digitally savvy, strong Data Privacy understanding •Distrustful of companies •Uncomfortable sharing data •Actively protect privacy	<b>High Awareness/No Protection – under 35</b>  •Digitally savvy, strong Data Privacy understanding •Trust companies •Comfortable sharing data •Seek convenience	<b>High Awareness/No Protection – over 35</b>  •Digitally savvy, strong Data Privacy understanding •Trust companies •Comfortable sharing data •Seek convenience

Each session included a 2-hour, full-group discussion, followed by a few one-on-one interviews.

#### Session flow:

- Warm up: Most used app and recollection of consent experience and the data agreed to share; data-sharing scandals in the recent news
- Consent exercise: Identify the important elements of consent: what data, what for, how long, who will get it, what do I get, etc.
- Data types: Discern if different types of data should require different consent experiences or different levels of granularity
- Consent use case testing: Displayed and discussed multiple consent flows to determine willingness to read and ability to understand, as well as willingness to consent to different programs. We tested multiple alternative approaches to consent, testing different levels of granularity and brand trust.

#### Hypotheses Tested

Hypotheses	Group One	Group Two	Group Three
The more educated a consumer is about how their data is being used by companies, the more concerned they become, and the more willing they are to take action to protect themselves.	<b>STRONGLY CONFIRMED</b>	<b>CONFIRMED</b>	<b>STRONGLY CONFIRMED</b>
Consumers prefer consent flows that are explicit, unbundled, revocable, simple, and time-bound compared to traditional T&Cs and Privacy Policies.	<b>STRONGLY CONFIRMED</b>	<b>STRONGLY CONFIRMED</b>	<b>STRONGLY CONFIRMED</b>
Consumers are more willing to invest in understanding and to grant consent when it is presented in a granular and consistent way.	<b>STRONGLY CONFIRMED</b>	<b>STRONGLY CONFIRMED</b>	<b>STRONGLY CONFIRMED</b>



Each hypothesis was confirmed in group discussions as well as by pre- and post-session questionnaires.

Hypothesis	Conclusion
<p><b>1.The more educated a consumer is about how their data is being used by companies, the more concerned they become, and the more willing they are to take action to protect themselves</b></p>	<ul style="list-style-type: none"> <li>• It was immediately evident in each group that the more consumers learned, the more concerned and protectionist they became</li> <li>• Post-session, participants showed a 20% decrease in overall comfort levels in digital data sharing</li> <li>• Post-session, participants showed a 23% increase in agreeing with the statement “it is worth investing time to understand why companies collect and use my data”</li> </ul>
<p><b>2.Consumers prefer consent flows that are explicit, unbundled, revocable, simple, and time-bound compared to traditional T&amp;Cs and Privacy Policies</b></p>	<ul style="list-style-type: none"> <li>• While no participants remembered what data they consented to share in their most-used mobile apps at the start of the sessions; consumers can be easily nudged to take more active responsibility in understanding data use</li> <li>• Consumers can distinguish between and care about the different types of data shared, sharing purposes, and companies sharing or using their data</li> </ul>
<p><b>3.Consumers are more willing to invest in understanding and granting consent when it is presented in a granular and consistent way</b></p>	<ul style="list-style-type: none"> <li>• Simple but detailed opt-in statements gave consumers</li> <li>• Comfort in sharing data because of clarity of use and control (e.g., revocation rights)</li> <li>• Increased likelihood of granting consent</li> <li>• Confidence that the data being shared will not be misused</li> </ul>

**Key Finding on consumer attitudes to consent management:**

1. Consumers overwhelmingly prefer explicit, unbundled, revocable, simple, and time-bound consent flows. Singapore and Australia Participants unanimously voted below as the best opt-in/ consent experience.

