Australian Government
The Treasury

TSY/AU

Privacy Impact Assessment

Consumer Data Right

March 2019

Manager
Media and Speeches Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: medialiaison@treasury.gov.au

Contents

Glossary

Abbreviation	Definition
ACCC	Australian Competition and Consumer Commission
AFCA	Australian Financial Complaints Authority
AIC Act	*Australian Information Commissioner Act 2010*
API	Application Programming Interface
APPs	Australian Privacy Principles
CALD	Culturally and linguistically diverse groups of people
CC Act	*Competition and Consumer Act 2010*
CDR	Consumer Data Right
CDR system	The regulatory system of legislation, rules and standards that creates and enlivens the rights of CDR consumers
Code	*Privacy (Australian Government Agencies – Governance) APP Code 2017*
DSB	Data Standards Body
EDR	External Dispute Resolution
GDPR	General Data Protection Regulation
OAIC	Office of the Australian Information Commissioner
OBR	Open Banking Review
ICCPR	The International Covenant on Civil and Political Rights
NERs	National Energy Rules
NERRs	National Energy Retail Rules
PC	Productivity Commission
PC Report	The Productivity Commission's Data Availability and Use Inquiry Report
PIA	Privacy Impact Assessment
Privacy Act	*Privacy Act 1988* (Cth)
Rules	Consumer Data Rules
Standards	Consumer Data Standards
Taskforce	Data Availability and Use Taskforce

Summary

Consumer Data Right background

The Consumer Data Right (CDR) provides individuals and businesses with a right to access data relating to them held by businesses (for example, raw bank transaction data) and 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.

The application of the CDR to the banking sector is referred to as Open Banking.

It is intended that improved consumer driven access to data will support better price comparison services, taking into account Australians' actual circumstances, and promote more convenient switching between products and providers. Improved access to data will also enable the development of better and more convenient products and services, customised to individuals' needs. Improved competition and data-driven innovation will support economic growth and create new high-value jobs in Australia. Better access to data will also support more efficient processes for businesses, with savings flowing through to Australian consumers.

However, the CDR is not merely an economic right. The CDR supports individuals' fundamental human right to privacy by enhancing their rights to access the personal data that businesses hold on them and obtain assistance in understanding that data. The CDR also enhances the privacy protections for data subject to its data portability regime.

Faster, more efficient and more convenient data access, in particular by third parties, can introduce new privacy threats and exacerbate existing threats.

The CDR framework therefore places a key focus on protecting individuals against privacy and security threats to their data.

Data that is transferred under the CDR will be subject to Privacy Safeguards, contained in the primary CDR legislation, which set minimum privacy protections. CDR data must also be provided in a manner which complies with consumer data rules (Rules) developed and enforced by the ACCC and mandated consumer data standards (Standards), which deal with matters such as information security.

The Office of the Australian Information Commissioner (OAIC) has a principle role of advising on and enforcing privacy protections in the CDR framework. The OAIC will be supported in systemic enforcement activities by the Australian Competition and Consumer Commission (ACCC). The framework introduces a range of avenues for individuals to seek meaningful remedies for breaches, including direct rights of action, External Dispute Resolution (EDR), and a 'no wrong door' approach for consumer complaints between regulators.

PIA Methodology and Stakeholder Consultation

This Privacy Impact Assessment (PIA) for the CDR was prepared by the Treasury in accordance with the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Code) and the OAIC *Guide to Undertaking Privacy Impact Assessments* (OAIC PIA guidance).[1] The PIA includes a detailed analysis of the threats involved with the implementation of the CDR and mitigation strategies, to support better management of those threats.

The OAIC PIA guidance does not prescribe a particular methodology for completing PIAs. This recognises that approaches may differ among agencies. Nevertheless, a common approach to conducting PIAs is to systematically assess the privacy impacts of the project against each of the APPs.

This PIA takes a different approach, more akin to a security Threat and Risk Assessment. It assesses the CDR regime using first principles of risk assessment. The approach taken reflects that the CDR regime incorporates its own Privacy Safeguards which are stronger than the APPs in a number of ways (discussed further below). Had we simply assessed the CDR regime against the APPs, the PIA would not have accurately drawn out the risks associated with the regime.

The PIA reflects the privacy impact analysis conducted as part of the development of the CDR policy including the outcomes of stakeholder consultations on privacy and information

[1] *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Code), available at: https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/privacy-australian-government-agencies-governance-app-code-2017 and Office of the Australian Information Commissioner, (2014) 'Guide to undertaking privacy impact assessment' (OAIC PIA Guidance), available at: https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf.

security issues. Stakeholders were heavily engaged at each stage of the CDR development, including through consultations run by the Productivity Commission (PC), the Taskforce which developed the Government's response to the PC's 2017 *Data Availability and Use Inquiry Report* (PC Report), the Open Banking Review (OBR), the Government's consultations on the report of the OBR, via the Government's consultation processes on the legislation for the CDR, and via the ACCCs consultation during rulemaking and the Data Standards Body's consultation during standards setting processes. The design of the CDR is heavily influenced by a range of views from consumer and privacy groups on the design of the CDR.

Given the fundamental importance of the right to privacy and other human rights to the operation of society, extensive consideration has been undertaken of the effects of the CDR on an individual's right to privacy during these phases of consultation.

This second version of the PIA has been developed based on the proposed regulatory framework for the CDR, incorporating key design decisions as part of rulemaking and standard setting processes, and public feedback on the first version of the PIA.

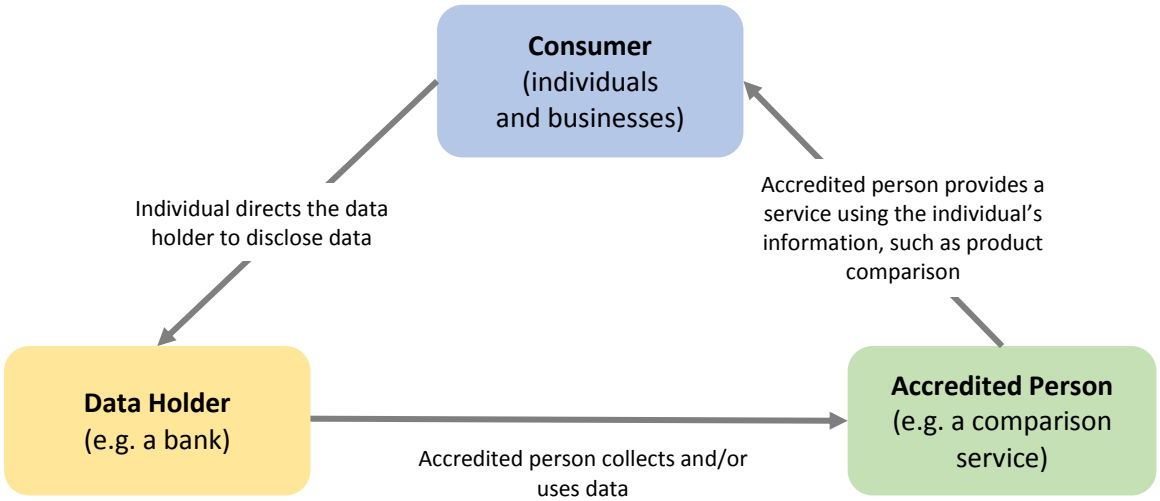
It should be noted that the PIA process is an iterative one, and this PIA has been undertaken at a relatively early stage of development of the CDR. Further privacy assessments will be required as part of future sector designation and rulemaking processes. In particular, a new or updated PIA should be prepared once all design features of the CDR are settled in advance of the launch of access to consumer data.

Mapping Personal Information

The transfer of an individual's personal data in the CDR involves multiple stages. A way to conceptualise the CDR is a simple model with an individual, a data holder and a data recipient.

The CDR information flow begins with a consumer engaging with a service provider who is an accredited data recipient. The consumer authorises them to collect data from a data holder. The consumer then authorises their data holder to disclose the data to that data recipient. The data recipient can then access the data in accordance with the terms of the access to which the consumer consented. The data recipient can only use, hold or disclose the data in accordance with any permissions given by the consumer. The data holder and recipient must comply with privacy and information security requirements set out by the

CDR regime. When all use permissions are spent, the data must be destroyed or de-identified.



The consumer may also request that the Data Holder transfer the information directly to the consumer themselves. There may be many more participants involved in the CDR system who add further complexity to the simple model outlined above.[2] These include intermediaries such as financial advisors, API providers, cloud storage services, data processing or filtering services, designated gateways and other accredited or non-accredited parties who may be operating domestically or internationally.

Impacts on Privacy and Risk Mitigation Strategies

As there are multiple stages and players involved in the CDR system, there are a number of potential privacy threats associated with the system. These threats may have consequences for the rights and wellbeing of individuals and businesses. These threats are broadly categorised into identification threats; transfer threats; collection, use or disclosure authorisation (genuineness) threats; authorisation (compliance) threats; holding threats; and data quality threats.

[2] In this document, references to a CDR participant mean anyone taking part in the CDR – it is not limited to the technical definition of CDR participant which is included in the *Treasury Laws Amendment (Consumer Data Right) Bill 2019.*

Within these categories, key privacy issues include: the threat of accredited entities not obtaining genuine consent; the threat of hacking activities or other cybercrimes; and the threat that entities will intentionally or unintentionally misuse the individual's personal data. Each of these critical threats may have consequences such as psychological and other physical harm, emotional distress, and financial or reputational loss. The likelihood and severity of these costs, however, will vary from case to case.

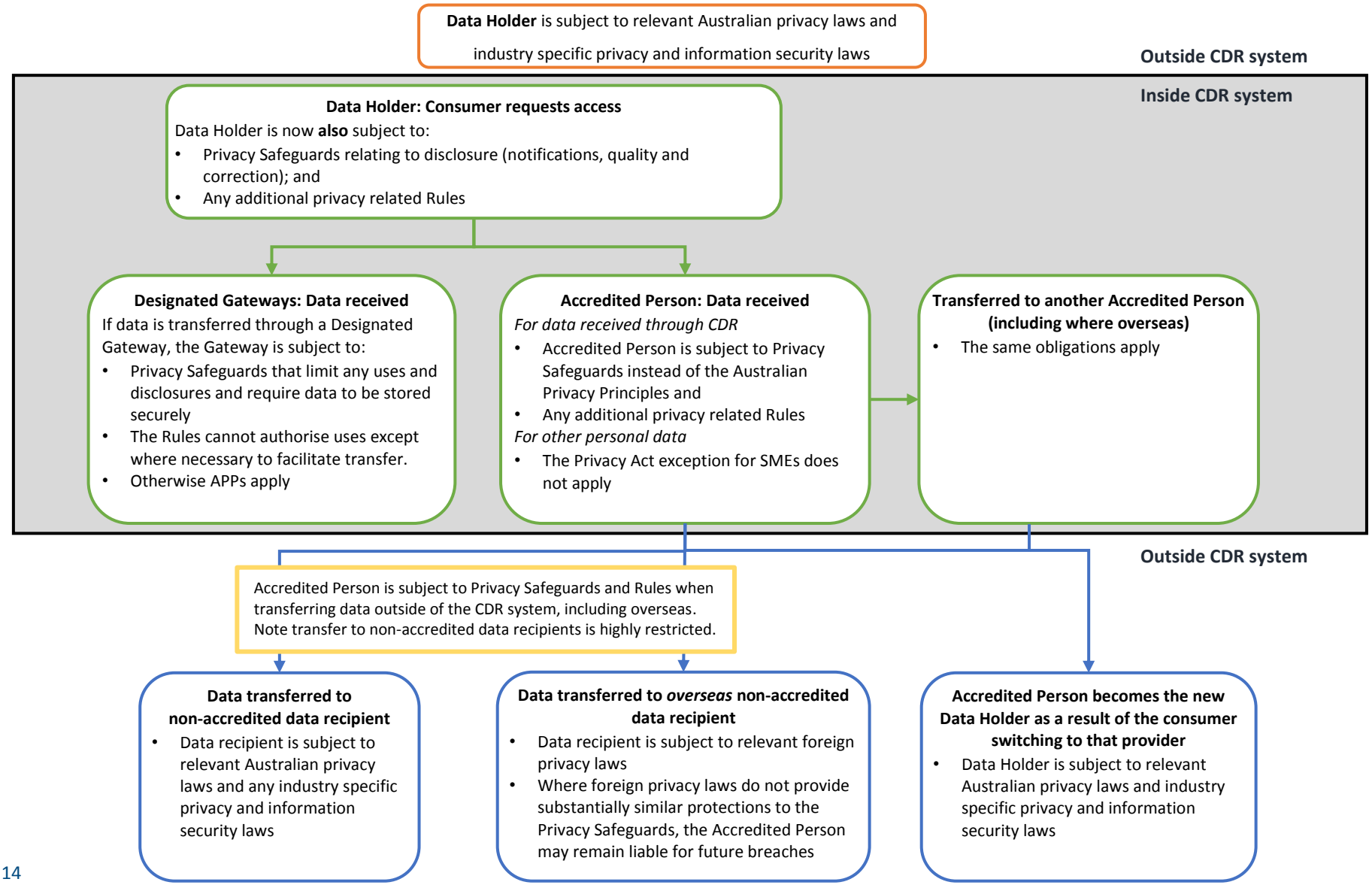
The CDR framework introduces a number of risk mitigation mechanisms to manage the potential threats. The CDR legislation, the Treasury Laws Amendment (Consumer Data Right) Bill 2019 (the Bill), expands on current privacy and security protections available under the *Privacy Act 1988* (Cth) (Privacy Act). These protections include: new Privacy Safeguards; applying the obligation to provide protections to a broader number of persons and datasets; powers for the OAIC and ACCC to ensure they can advocate for privacy and consumers; technical Standards; Rules providing for genuine consent and use restrictions; an accreditation register; external dispute resolution; and direct rights of action. Protections in the CDR are intended to provide a higher level of privacy protection than those existing under the Australian Privacy Principles (APPs) and the Privacy Act. A high-level comparison of the APPs and the CDR Privacy Safeguards is in the table below (a more detailed comparison is at Appendix A). The diagrams below illustrate the privacy protections that apply at each stage of the CDR information flow.

Table 1: Australian Privacy Principles and CDR Privacy Safeguards

Australian Privacy Principle (APP)	CDR Privacy Safeguard
APP 1 – open and transparent management of personal information	Privacy Safeguard 1 – Equivalent
APP 2 – anonymity and pseudonymity	Privacy safeguard 2 – Stronger
APP 3 – collection of solicited personal information	Privacy safeguard 3 – Stronger
APP 4 – dealing with unsolicited personal information	Privacy safeguard 4 – Stronger

APP 5 – notification of the collection of personal information	Privacy safeguard 5 – Stronger
APP 6 – use or disclosure of personal information	Privacy safeguard 6 – Stronger
APP 7 – direct marketing	Privacy safeguard 7 – Stronger
APP 8 – cross-border disclosure of personal information	Privacy safeguard 8 – Equivalent, with one addition
APP 9 – adoption, use or disclosure of government related identifiers	Privacy safeguard 9 – Stronger
	Privacy safeguard 10 – No APP equivalent
APP 10 – quality of personal information	Privacy safeguard 11 – Equivalent
APP 11 – security of personal information	Privacy safeguard 12 – Equivalent
APP 12 – access to personal information	The CDR as a whole is the equivalent of APP12.
APP 13 – correction of personal information	Privacy safeguard 13 – Equivalent

Privacy Protections at Each Stage



Australian Bank

- Australian Privacy Principles (if applicable)
- Only those Privacy Safeguards relating to disclosures under the CDR (notifications, data quality and correction rights)
- Privacy related Rules

Accounting Software Provider (Accredited Person)

- For data received through the CDR:
  - Privacy Safeguards
  - Privacy related Rules
- For other personal data:
  - Privacy Act (exception for SMEs does not apply)

Accountant (Non-Accredited)

- Australian Privacy Principles (if applicable)
- Accredited persons are subject to Privacy Safeguards and Rules when transferring to non-accredited persons

Foreign Accountant (Foreign Non-Accredited)

- Foreign privacy laws
- Where foreign privacy laws do not provide substantially similar protections to the Privacy Safeguards, the Accredited Person who transferred the data may remain liable for future breaches
- Possibly, Australian Privacy Principles
- Accredited persons are subject to Privacy Safeguards and Rules when transferring to non-accredited persons

Recommendations & Conclusion

This PIA highlights a range of privacy threats. Some of these threats could lead to substantial financial, personal and emotional loss. However, the framework includes privacy protections to mitigate these privacy threats. The CDR simultaneously offers individuals corresponding benefits to privacy, competition, convenience and choice.

The PIA makes a number of recommendations in respect of the implementation of the proposed mitigants, to ensure key elements of the CDR system that protect individuals' privacy and security meet their objectives. The recommendations are summarised in the table below.

Table 2: Privacy Impact Assessment Recommendations

Recommendation	Description
Recommendation 1	The ACCC, the OAIC and the Data Standards Body should continue to incorporate behavioural research into the design of the CDR system to ensure that the system works effectively and takes into account *actual* consumer preferences and behaviours regarding the exercise of their privacy rights. Ongoing consumer testing by the Data Standards Body, and the pilot program to test the performance, security and reliability of the CDR system, should have particular regard to vulnerable consumer groups. Test groups should be of sufficient size and diversity to provide justified confidence in the safety of consent processes.
Recommendation 2	The ACCC, the OAIC and the Data Standards Body should ensure that their annual reporting includes reporting on the operation of the CDR, particularly relating to privacy, to provide assurance that rules and practices continue to appropriately handle privacy threats. To facilitate this, the ACCC may consider compiling a consolidated annual CDR report, based on the reporting of relevant agencies' CDR functions.

Recommendation 3	The ACCC should continue to work with the OAIC to ensure that the Rules create a consent framework that ensures consent is genuine, and protects vulnerable individuals.
Recommendation 4	When designing and implementing the Rules and data security and transfer Standards, the ACCC and the Data Standards Body should seek to avoid placing undue weight on the benefits of competition and innovation at the expense of protecting privacy. It is noted that there is not always a trade-off between these objectives. Strong privacy protections will drive confidence in the system – which is a necessary prerequisite for realising all other objectives. Additionally, the data standards working groups should increase transparency around the extent to which privacy-by-design is incorporated into their processes. The working groups should commit to periodic review of the API specifications, and be prepared to specify more granular APIs should inadvertent information disclosure become a concern.
Recommendation 5	The ACCC and the Data Standards Body should continue to work with the OAIC to ensure that the privacy related Rules and Standards remain largely consistent across designated sectors, with tailoring to particular privacy risks where necessary.
Recommendation 6	The ACCC should consider making rules requiring accredited data recipients to put in place processes to ensure that CDR data held by the data recipient is not inappropriately accessed by the data recipient's employees.
Recommendation 7	The Treasury, the ACCC, the OAIC and the Data Standards Body should continue to coordinate their activities, and put in place information sharing arrangements and memoranda of

	understanding as appropriate.
Recommendation 8	The CDR education program should include a focus on raising CDR participant awareness of privacy threats and rights.
Recommendation 9	The post-implementation assessment of Open Banking, and the CDR for future designated sectors, should report specifically on privacy relevant metrics such as privacy related complaints and data breaches. Arrangements should be put in place at commencement so that the post-implementation assessment can be conducted with the benefit of a robust evidence base.
Recommendation 10	All significant changes to the CDR legislation or Rules should be accompanied by further PIAs, conducted in accordance with the OAIC *Guide to undertaking privacy impact assessments* and following engagement with privacy and consumer representatives.

The Consumer Data Right

The CDR seeks to give individuals and businesses the right to safely access data that relates to them that is held by businesses. Through the CDR, individuals and businesses will also be able to direct that a data holder release their data to an accredited data recipient. The scope of the CDR will encompass data relating to an individual who is identifiable or reasonably identifiable, as well as data that does not relate to an identifiable or reasonably identifiable CDR consumer, for example product data.

While provision of access to data and data sharing is already occurring in various sectors, the objective of the CDR is to provide a framework that makes data sharing at the consumer's request easier and safer in designated sectors. Work is already underway to implement the CDR in the banking sector following the OBR, and the Government has announced that energy and telecommunications will be the next sectors to which the CDR will be applied. Over time, the CDR will be applied to further sectors on a sector-by-sector basis.

Timing

In implementing the CDR, it is important to ensure that the security and privacy of consumers' data is paramount and that personal data will be able to be accessed or used under the regime only with the consumer's consent. To ensure the long term success of the regime, a phased implementation has been adopted.

This will provide additional time for the development of consent requirements and processes, and for subsequent consumer testing of consent processes.

- From 1 July 2019, major banks will be required to publicly share product data about credit and debit cards, deposit accounts and transaction accounts.
- Also from 1 July 2019, the ACCC and Data 61 will launch a pilot program with the big four banks to test the performance, reliability and security of the Open Banking system.
    - Consumers and FinTechs will be invited to participate in these pilots and the ACCC and Data61 will also work closely with other banks who have expressed an interest in participating in Open Banking earlier than originally envisaged.

    - This will include extensive consumer and beta testing of access arrangements, including consent processes. It is important to ensure that test groups are of sufficient size and diversity to provide justified confidence in the safety of consent processes, with particular regard for vulnerable consumer groups.
- Once the ACCC is comfortable with the robustness of the system, banks will publicly share consumer data about credit and debit cards, mortgages, deposit accounts and transaction accounts, which will be no later than 1 February 2020.
- On 1 February 2020, product data for mortgage accounts will be made available.
- From 1 July 2019, the ACCC will begin formally engaging with parties interested in accreditation.

Remaining banks will begin sharing consumer and product data about credit and debit cards, deposit accounts and transaction accounts from 1 July 2020 and will be given a 12-month delay on timelines for remaining data sets compared to the major banks.

Background and Rationale for Consumer Data Right

Data access and use rights have been explored in Australia through multiple reviews and inquiries. The 2014 *Financial System Inquiry*,[3] the 2015 *Competition Policy Review*,[4] the 2016 House of Representatives Standing Committee on Economics' *Review of the Four Major Banks: First Report* (Review of the Four Major Banks),[5] and the 2017 *Independent Review into the Future Security of the National Electricity Market: Blueprint for the Future* (Finkel

[3] David Murray, Kevin Davis et al, 'Financial System Inquiry' (2014) available at: http://fsi.gov.au/.

[4] Ian Harper, Peter Anderson et al, 'Competition Policy Review' (2015) available at: http://competitionpolicyreview.gov.au/.

[5] House of Representatives Standing Committee on Economics, 'Review of the Four Major Banks: First Report' (2016) available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Economics/Four_Major_Banks_Review/Report.

Review)[6] all recommended that Australia examine or develop improved arrangements for individuals to access and transfer their information in a useable format.

Table 3: Background to the Consumer Data Right

Inquiry	Recommendation
Financial System Inquiry	**Recommendation 19: Data access and use** • Review the costs and benefits of increasing access to and improving the use of data, taking into account community concerns about appropriate privacy protections.
Competition Policy Review	**Recommendation 21: Informed choice** • Governments should work with industry, consumer groups and privacy experts to allow consumers access to information in an efficient format.
Review of the Four Major Banks	**Recommendation 4** • The committee recommends that Deposit Product Providers be forced to provide open access to customer and small business data by July 2018. ASIC should be required to develop a binding framework to facilitate this sharing of data, making use of Application Programming Interfaces (APIs) and ensuring that appropriate privacy safe guards are in place. Entities should also be required to publish the terms and conditions for each of their products in a standardised machine-readable format. • The Government should also amend the *Corporations Act 2001* to introduce penalties for non-compliance.
Finkel Review	**Recommendation 6.3** • By mid-2020, the COAG Energy Council should facilitate measures to remove complexities and improve consumers' access to, and rights to share, their energy data.

[6] Dr Alan Finkel, Karen Moses et al, 'Independent Review into the Future Security of the National Electricity Market: Blueprint for the Future' (2017) available at: https://www.energy.gov.au/government-priorities/energy-markets/independent-review-future-security-national-electricity-market.

Productivity Commission Inquiry into Data Availability and Use

The Productivity Commission provided its final report to the Government on 31 March 2017 and it was tabled in Parliament on 8 May 2017.

The PC recommended the creation of an economy-wide Comprehensive Data Right (Recommendation 5.1). The PC considered that consumer data must be provided on request to consumers or directly to a designated third party in order to allow consumers to exercise a number of rights. This was summarised as the 'Comprehensive Right to access and use digital data' (Comprehensive Right), which would enable consumers to:

- share in perpetuity joint access to and use of their consumer data with the data holder;
- receive a copy of their consumer data;
- request edits or corrections to the data for reasons of accuracy;
- be informed of the trade or other disclosure of consumer data to third parties; and
- direct data holders to transfer data in machine-readable form, either to the individual or to a nominated third party.

The PC recommended that where a transfer is requested outside of an industry (such as from a medical service provider to an insurance provider) and the agreed scope of consumer data differs between the source industry and the destination industry, the scope that applies should be that of the data sender.

The Comprehensive Right was directed at improving consumer outcomes by enabling individuals to better assess the value of prospective and existing services and encourage switching.

On 26 November 2017, in response to the PC's recommendation, the Government announced that the CDR would be implemented as a measure for individuals to harness their digital data, initially in the banking, energy and telecommunications sectors, with its design to be informed by the OBR.

On 1 May 2018, in its full response to the PC's report, the Government reiterated its commitment to the creation of the CDR.

Review into Open Banking in Australia

In the 2017-18 Budget the Government announced that it would introduce an Open Banking regime in Australia. On 20 July 2017, the Treasurer commissioned an independent review, headed by Mr Scott Farrell, to recommend the best approach to implement such a regime.

This review made 50 recommendations in relation to the legal and regulatory arrangements for the economy-wide CDR, and more specifically, how it should be applied to banking data.

On 9 May 2018, the Government announced its plan for Open Banking and the CDR, accepting the Open Banking Review's (OBR) recommendations regarding the design of the CDR, with implementation to be phased in from July 2019.

Current data sharing practices

Community attitudes to privacy

A summary of key findings of the OAIC 2017 'Australian Community Attitudes to Privacy Survey' (ACAPS) and the Consumer Policy Research Centre's Report 'Consumer data & the digital economy' (CPRC data report) is provided below.[7] Both reports were influential in the CDR policy design process. At a high level, these reports suggest Australians are concerned about their privacy, and the way their personal information is being used. However, many have an incomplete understanding of Australian privacy law and frameworks, and few consistently read the privacy policies of the organisations with which they engage.

2017 ACAPS

The OAIC conducts the ACAPS approximately every 5 years. The 2017 survey allowed respondents to select different types of personal information they would be reluctant to provide. This resulted in the survey finding that 42 per cent of respondents were reluctant to provide their financial status information to organisations, and 34 per cent of respondents

[7] Jayne Van Souwe, Patrick Gates, et al , 'Australian Community Attitudes to Privacy Survey 2017' (2017), Office of the Australian Information Commissioner, available at: https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017; Phuong Nguyen and Lauren Solomon, 'Consumer data and the digital economy: Emerging issues in data collection, use and sharing' (2018), Consumer Policy Research Centre, page 4, available at: http://cprc.org.au/2018/07/15/report-consumer-data-digital-economy/.

were reluctant to provide their contact information. Both of these are data sets that are expected to be included in the CDR.

Of the respondents who indicated they were reluctant to provide personal information: 17 per cent were mainly reluctant due to the fear that doing so would lead to financial loss or allow people to access their bank account; 16 per cent for privacy preservation reasons; 15 per cent due to the fear that the information would be misused or passed on without their knowledge; and 13 per cent due to security concerns.

Only 11 per cent of respondents were comfortable with businesses sharing their information, though younger respondents were more comfortable than older respondents. Perceived misuses of information included: organisations that respondents hadn't dealt with directly getting hold of their personal information (87 per cent); an organisation revealing one customer's information to other customers (87 per cent); information being used by an organisation for purposes that differ from the purposes for which the information was given to the organisation (85 per cent); organisations monitoring respondents' activities online (84 per cent); organisations seeking information that is not relevant to the purpose of the transaction (81 per cent); and organisations sending data overseas (74 per cent).

It is clear that Australians' trust in organisations that hold their data differs depending on the organisation and mode of interaction: 59 per cent of respondents considered financial institutions to be trustworthy with regard to how they protect or use personal information; 34 per cent considered organisations providing technology products to be trustworthy; and 12 per cent considered the social media industry to be trustworthy. 83 per cent of respondents think there are greater privacy risks dealing with organisations online than offline.

Though Australians are concerned about their privacy, only 37 per cent of respondents were aware they could access their personal information from government and businesses, only 18 per cent responded that they always read privacy policies, and only 13 per cent refuse to deal with an organisation because of privacy concerns.

In respect of incidents of identity theft, 11 per cent of respondents reported that they had been a victim of identity fraud or theft in their lifetime.

It is worth noting that for many of the above results, education levels affected the likelihood that a respondent would either be aware of their privacy rights, or would take steps to protect their own privacy.

CPRC data report

The CPRC was established by the Victorian Government in 2016 as an independent research organisation, to undertake research to inform policy reform and business practice changes to improve outcomes for consumers. The CPRC data report analyses a range of data practices in Australia today. As part of this report, the CPRC commissioned Roy Morgan to survey a nationally representative sample of 1004 Australians to examine their understanding of consent to data collection, use and sharing when accessing products and services. Consumers were asked questions relating to their online behaviour, knowledge and attitudes regarding data collection practices, and their expectations around consumer protection and data control.[8]

Key findings of this research include that 91 per cent of respondents are aware that companies have the ability to follow their activities across websites, 88 per cent are aware that companies exchange information about their customers with third parties for purposes other than delivering the product or service. Six per cent of respondents reported that they read the Privacy Policies or Terms & Conditions for all the products and services they signed up to in the past 12 months, and 33 per cent reported that they never read these documents in the past 12 months.

Of the 67 per cent of respondents who reported having read a Privacy Policy or Terms and Conditions in the past 12 months, 67 per cent indicated that they signed up to receive the product or service even though they did not feel comfortable with the policies.

Reasons given included that it was the only way to access the product or service (73 per cent), that they trusted the company would not misuse their data (23 per cent), that

[8] Phuong Nguyen and Lauren Solomon, 'Consumer data and the digital economy: Emerging issues in data collection, use and sharing' (2018), Consumer Policy Research Centre, page 4, available at: http://cprc.org.au/2018/07/15/report-consumer-data-digital-economy/.

they believed Australian law would prevent the misuse of their data (20 per cent), and that nothing bad has happened to them in the past (18 per cent).

Like the 2017 ACAPS, this research indicates that trust may vary depending on the company, with participants in focus groups suggesting they are less likely to read these documents when dealing with larger and more reputable companies.

Also like the 2017 ACAPS, the CPRC report found that at least 61 per cent of respondents were uncomfortable with most types of information being shared with third parties for secondary purposes. 61 per cent were uncomfortable with their name being shared, 69 per cent were uncomfortable with their purchase history being shared, and 86 per cent and 87 per cent respectively were uncomfortable with their messages and phone contacts being shared.

The CPRC report asked respondents a range of questions about data use and expectations of companies that were not asked in the 2017 ACAPS.

While all findings were influential, key findings include that 95 per cent of respondents agreed that companies should give options to opt out of certain types of information they collect, how it can be used, and/or what can be shared, 92 per cent agreed companies should be open about how they use data to assess eligibility for products or services, 91 per cent agreed that companies should only collect information currently needed for providing their product or service, and 77 per cent disagreed with the statement 'If I trust a company, I don't mind if it buys information about me from database companies without asking me'.

Impact on policy design

The above results led to the following key high-level assumptions, which influenced design decisions throughout the CDR policy design process:

- a sizeable proportion of Australians are concerned about the privacy of their personal information, and are particularly concerned where that information is financial information;
- privacy for the sake of privacy is of value to an equal proportion of Australians as privacy for the sake of prevention of financial loss;

- in allowing information to be shared through the CDR, it is possible that information will be disclosed from a data holder who is considered trustworthy by the majority of Australians, to a data recipient who is not considered trustworthy;
- very few Australians consistently read privacy policies or have a great deal of awareness of their privacy rights;
- many Australians do not fully understand what types of information are currently being collected and shared about them, but they want to be enabled to understand and have a voice in the decision making process; and
- persons with lower levels of education, persons who are members of culturally and linguistically diverse (CALD) groups, or persons who experience intellectual disabilities are less likely to be aware of their privacy rights and to take actions to protect their privacy.

More detailed findings of these reports were also highly influential in relevant areas.

It should be noted that healthy cynicism by consumers regarding the potential uses and safety is itself a significant privacy risk mitigant, provided that the proposed data portability gives them genuine informed control over their data.

Data sharing

Data sharing is not a new practice in Australia – in particular in the banking and energy sectors.

For example:

- Credit providers provide information to credit reporting agencies under the regime contained in Part IIIA of the Privacy Act;
- Banks enter into bilateral agreements with select data-driven service providers (such as accounting software providers) to share data;
- Third party service providers, with the consent of consumers, access data through screen-scraping technologies; and
- There are existing consumer data rights under the National Electricity Rules and National Electricity Retail Rules.

Bilateral agreements between banks and partner companies are negotiated individually between the parties. This approach can be inefficient, time-consuming and expensive for data seekers to engage in. The terms of these agreements may also lack transparency and control for the consumer.

There have also been some recent initiatives to increase data sharing between banks and FinTech companies of non-customer specific data sets, such as data on branch and ATM locations and on foreign exchange rates.

Australia's energy regulatory framework includes a rule which empowers customers and authorised third parties to obtain a consumer's electricity consumption data from distribution network service providers and retailers and establishes minimum requirements related to the format, timeframes and reasonable charges for providing the data. Individuals were granted this right on 6 November 2014. This original consumer energy data right was amended in 2015 as part of changes to Chapter 7 of the National Energy Rules (NERs), to facilitate competition in metering. The energy electricity data right is set out in the NERs and the National Energy Retail Rules (NERRs), and gives individuals the right to access their metering data and a right to authorise third-party representatives to access the data on their behalf.

There are also a number of currently unregulated approaches to data sharing, of which screen-scraping is one example. Screen-scraping involves the customer providing their login credentials to a third party who uses them to access the data holder's customer-facing website. Data is then collected from the website. Concerns have been raised about heightened fraud and privacy threats associated with such unregulated methods, including during consultations conducted by the OBR.

Most of the threats identified in this PIA exist in relation to these and other existing data sharing channels. These channels will continue to exist in parallel to the CDR. The CDR is not therefore a replacement 'pipe' but is instead intended to be a safer pipe.

Data collection

Individuals' data is also already being collected in a number of ways, including via: cookies; web beacons and pixel tags; device information and tracking; 'fingerprinting' (using a combination of specific data from devices or browsers as 'fingerprints' to recognise users);

and payment cards and loyalty cards.[9] In addition, data brokers collect and aggregate information from commercial, government and other publicly available sources, from which they can derive inferred data about individuals.

Objectives of the Consumer Data Right

Benefits to privacy

Data access and portability rights have a dual nature, having both fundamental human rights and economic rights aspects.

As discussed above, access to data about oneself has been recognised internationally as a key component of an individual's human rights.

In Australia, the CDR acts as an expansion of APP 12 in respect of its provision of rights for individuals and provides a framework to make it easier for individuals to access their data in an environment with built-in privacy and security protections.

The direct right of access it affords corresponds directly with those granted under APP 12. APP 12 provides a right of access, requiring an APP entity to give an individual access to personal information about them on the request of the individual within a reasonable period, in the manner requested by the individual if it is reasonable or practicable to do so. However, there are a number of exceptions to this right. The CDR grants additional access rights to those contained in APP 12, in relation to designated data sets. It seeks to provide greater functionality and more security than existing privacy rights. It may also apply to different kinds of data than do those rights.

However, with increasing complexity and volumes of data held on individuals, a right to directly access data may not be a *meaningful* privacy right due to limits on the ability of individuals to understand the data (or become aware of the implications that the holding of that data has for their rights).

---

[9] Phuong Nguyen and Lauren Solomon, 'Consumer data and the digital economy: Emerging issues in data collection, use and sharing' (2018), Consumer Policy Research Centre, pages 11-15, available at: http://cprc.org.au/2018/07/15/report-consumer-data-digital-economy/.

The CDR grants additional access rights in relation to designated data sets by enabling individuals to give direct access to their data to third parties. It is partially intended to enable the development of third party services that may enhance privacy rights, by helping individuals to understand what data is held by businesses and understand and manage collection, use and disclosure permissions.

For example, it is expected to facilitate the development of 'data wallets', and new consent management services are already emerging under the UK Open Banking regime.

The expansion of access rights in this way (domestically and internationally, such as in Article 20 of the European General Data Protection Regulation (GDPR)) can be seen as part of the natural evolution of privacy rights in response to the changing nature of data holding in a digital society.

The CDR will introduce strict rules about the provision of informed, unbundled and explicit consent which may be expected to increase the level of public awareness and expectations regarding privacy consents generally.

The CDR is also intended to provide an alternative to existing data sharing methods with their associated privacy threats (for example, identity theft and fraud). It can be viewed as a safer 'pipe' for data portability.

In relation to this third party data access, the reforms impose an enhanced privacy framework beyond that which would ordinarily apply, directed at preventing inappropriate collection, disclosure, holding and use of data. Further details on the features of the CDR that seek to protect privacy and mitigate privacy risks are provided in the Risk Mitigation section below.

Consumer confidence is a prerequisite for success for data service providers in a system which depends on obtaining consumer consents to collect, use and disclose data. Data safety is a key selling point for their services. Commercial incentives may therefore strongly align with improved data safety and privacy protections.

Finally, the CDR expands the application of the Privacy Act to entities who are accredited under the CDR. This narrows the current exemption in the Privacy Act for small to medium enterprises and expands the scope of participants accountable for data protection.

Benefits to information security

The CDR is intended to achieve stronger privacy protections by improving information security in data sharing practices. The CDR regulatory framework involves the development of technical Standards that will require the use of API technology, digital identification of data recipients and encryption for data transfer. It will also impose privacy and information security obligations on data recipients for data received under the CDR.

The CDR will therefore encourage the development of new data technologies and systems that are likely to increase the safety of data flows and holdings.

As outlined above, data is already being shared via unregulated methods, such as screen-scraping. The use of API technology implies fewer security risks than many of these existing methods.

Economic benefits

In addition to the increases in privacy and security protections outlined above, the CDR is expected to generate economic benefits via increased competition, convenience and individual choice.

The economic character of data rights arises in part because availability of information about oneself aids informed economic decisions.

By improving access to data, the CDR is aimed at simplifying product comparisons and increasing an individual's ability to either negotiate better offers with their current providers or switch products. Such practices encourage efficient switching behaviour and deliver economic benefits in the form of increased competition, and potentially lower prices, in designated sectors.

Over the longer term, improving customer control, choice and convenience is intended to promote a customer-centric data sector that will support the development of products and services that are tailored to individuals' needs. The development of this new sector could help drive innovation, economic growth and employment, and improve and expand the suite of services available to individuals and businesses.

Improvements in existing products and services will help to inform individuals about the best offers available to them, make everyday transactions more convenient, and contribute to consumer literacy. Some examples of expected improvements include:

- comparison tools for credit cards and mortgages, with product recommendations tailored to individuals' actual spending and repayment patterns;
- budgeting tools that show individuals all their financial products on one screen and help them better manage their finances by providing insights into current spending habits;
- analysis tools that use the level and timing of a household's energy usage to help them to determine the net benefits of investing in solar power and the size and type of system that would best suit them; and
- comparison tools that help individuals locate the best mobile phone and internet service provider deal for them, based on their actual mobile phone and internet data usage.

The CDR is also intended to reduce regulatory and security costs for individuals and businesses.

It is also intended to support improved compliance with regulations, including those directed at protecting individuals. For example, in the banking sector, it may assist credit licensees to comply with responsible lending obligations. These obligations provide that credit licensees must not enter into a credit contract with an individual, suggest a credit contract to them, or assist them to apply for a credit contract, unless the credit contract is suitable for the individual. In order to assess whether a credit contract is suitable for an individual, credit licensees must make reasonable inquiries about the individual's financial situation. By facilitating individual-driven sharing of data, the CDR may improve credit licensees' ability to verify the individual's financial situation.

The CDR's impact on economic rights may indirectly affect, and possibly promote, other human rights – such as rights to sustenance, housing and security.

Regulatory framework governing the Consumer Data Right

The CDR creates a new framework to enable individuals to more effectively use data relating to them for their own purposes.

The framework will enable individuals to direct the data holder to provide their data, in a CDR compliant format, to accredited entities. It will also allow individuals to access their data directly.

The CDR will provide the ACCC with the power to make Rules, in consultation with the OAIC, to determine how the CDR will function within each sector.

Entities must be accredited before they are able to receive CDR data relating to individuals and businesses. This will ensure that the accredited entities have satisfactory privacy and security safeguards before receiving data.

Under the CDR, data must be provided in a format and in a manner which complies with the Standards. While the Standards may apply differently across sectors, it is important that the manner and form of the data coming into the CDR system be consistent within and between designated sectors, as far as is practicable. This will promote interoperability, reduce costs of accessing data and lower barriers to entry by data driven service providers – promoting competition and innovation.

The right can be extended to additional sectors of the economy over time, following sectoral assessments by the ACCC in conjunction with the OAIC.

Privacy Safeguards

Data that relates to an individual will be subject to new Privacy Safeguards once an individual requests its transfer to an accredited recipient. The Privacy Safeguards are contained in the primary CDR legislation, setting the minimum privacy protections under the CDR.

The Privacy Safeguards are as follows:

Privacy safeguard 1—open and transparent management of CDR data

This safeguard ensures that individuals understand how their data is being handled by a data holder or accredited entity. The safeguard requires the CDR entity to make transparent policy and procedure documents about management of the CDR data available, and also provides individuals with the ability to raise any issues with the CDR participant.

CDR Privacy Safeguard 2 – Anonymity and pseudonymity

This safeguard will give an individual the option to use a pseudonym or remain anonymous when transferring information if it is appropriate to do so in the designated sector. As is the case with the similar APP 2, an individual may choose to use a pseudonym or remain anonymous using this Privacy Safeguard and still be reasonably identifiable and subject to protections within that situation.

CDR Privacy Safeguard 3 – Collecting solicited CDR data

This safeguard protects individuals from the unsolicited collection of CDR data. The individual must give a valid request for the accredited person to collect their data.

CDR Privacy Safeguard 4 – Dealing with unsolicited CDR data

This safeguard requires that an accredited person that finds itself in possession of CDR data without having requested that data must destroy that data, unless an Australian law requires it to retain the data.

CDR Privacy Safeguard 5 – Notifying the collection of CDR data

This safeguard ensures that an accredited person must notify an individual about the collection of their data under the CDR.

CDR Privacy Safeguard 6 – Use or disclosure of CDR data

This safeguard requires that an accredited data recipient or designated gateway must obtain consent from the relevant individual in accordance with the Rules before using or disclosing the CDR data.

CDR Privacy Safeguard 7 – Use or disclosure of CDR data for direct marketing by accredited data recipients

This safeguard ensures that individuals are not subject to unwanted direct marketing as a result of their engagement with the CDR system unless the use of the data for direct marketing purposes is allowed by the Rules or allowed under other Australian law or by a court/tribunal order.

CDR Privacy Safeguard 8 – Cross-border disclosure of CDR data by accredited data recipients

This safeguard protects individuals by providing that CDR data may only be disclosed by an accredited data recipient to a recipient who is located outside Australia and is not a CDR consumer for that CDR data where:

- the new recipient is an accredited data recipient; or
- if the CDR data is personal information about an individual – the accredited data recipient takes reasonable steps to ensure the new recipient does not breach the APPs (other than APP 1) in relation to the CDR data; or
- the accredited data recipient reasonably believes: that the new recipient is subject to a law, or binding scheme, that provides at least as much protection for the CDR data as the Australian Privacy Principles provide for personal information; and that a CDR consumer for the CDR data will be able to enforce those protections provided by that law or binding scheme.

CDR Privacy Safeguard 9 – Adoption or disclosure of government related identifiers

This safeguard provides that an accredited data recipient may not use or disclose government related identifiers, such as a tax file number, to identify an individual, except where the use is allowed under other Australian law or by a court/tribunal order.

CDR Privacy Safeguard 10 – Notifying of the disclosure of CDR data

This safeguard requires a data holder or an accredited data recipient to notify the individual that they have responded to a valid request to disclose the individual's CDR data.

CDR Privacy Safeguard 11 – Quality of CDR data

This safeguard requires CDR participants to take reasonable steps to ensure that the CDR data disclosed is accurate, up to date and complete for the purpose for which it is held. This safeguard applies to both data holders and accredited data recipients and requires that the individual is notified of any incorrect disclosures of data. It gives individuals the ability to require the CDR participant to disclose corrected CDR data.

CDR Privacy Safeguard 12 – Security of CDR data

This safeguard requires that an accredited data recipient or designated gateway protects CDR data from misuse, interference and loss as well as from unauthorised access, modification or disclosure. It also requires that any data that is no longer needed by an accredited data recipient or designated gateway for permitted purposes is either destroyed or de-identified in line with the Rules.

CDR Privacy Safeguard 13 – Correction of CDR data

This safeguard provides an individual with the ability to request that the data holder correct data following a valid request to disclose the data, and to request that an accredited recipient of the data correct the data.

The Safeguards provide consistent protections for consumer data of both individuals and small business consumers, and places requirements on CDR participants that are more restrictive than the requirements of the Privacy Act (outlined below).

The Privacy Act distinguishes between personal information and sensitive information, with sensitive information accorded a greater level of protection. The CDR does not make this distinction, and treats all information at least at the level of sensitive information.

In addition to the Privacy Safeguards, the framework provides flexibility to respond to emerging privacy threats, through the rulemaking and standard setting processes.

The ACCC may make additional Rules regarding the transfer, holding and use of data within the system, to build upon the Privacy Safeguards.

The Chair of the Data Standards Body, with assistance from that Body, may make technical standards, for example, information security standards, to support the operation of the Privacy Safeguards and any further privacy protections in the Rules. The Rules will mandate compliance with the standards. The standards apply as a contract between each data holder to which a binding standard applies, and each accredited person.

The CDR will give the OAIC the power to enforce the Privacy Safeguards and provide individual remedies to individuals, while the ACCC will have the function of enforcing the Rules and offence provisions, and for taking strategic enforcement actions.

All individual and small business customers in a designated sector are to have access to CDR-compliant dispute resolution processes, as required under the Rules, to resolve disagreements with participants in the system. It is envisaged that individuals will also have access to existing sector-specific alternative dispute resolution arrangements, for example the Australian Financial Complaints Authority (AFCA).

Privacy and Other Rights

The right to privacy

The right to privacy is a human right, inherent in the basic dignity of the individual. It is protected under Article 12 of the United Nations Universal Declaration of Human Rights, which provides that:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.* [10]

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) replicates this provision, qualifying it to protect against 'unlawful' attacks upon honour and reputation. [11]

The UN Human Rights Committee has not defined 'privacy', but it is generally understood to comprise freedom from unwarranted and unreasonable intrusions into activities that society recognises as falling within the sphere of individual autonomy. This includes personal data. It has been suggested that there are four facets of the right to privacy:

- Information Privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records;
- Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches;

[10] Available at: http://www.un.org/en/universal-declaration-human-rights/.

[11] Available at: http://www.un-documents.net/iccpr.htm.

- Privacy of communications, which covers the security and privacy of mail, telephones, email and other forms of communication; and
- Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.[12]

In its 2008 Report, '*For Your Information: Australian Privacy Law and Practice*', The Australian Law Reform Commission viewed privacy as 'the bundle of interests that individuals have in their personal sphere free from interference from others', and noted that 'privacy interests unavoidably will compete, collide and coexist with other interests'.[13] The Commission emphasised that 'compliance with basic information privacy principles … accords with commercial best practice standards.'[14]

The right to freedom of opinion and expression

The right to freedom of opinion and expression, protected under Article 19 of the ICCPR, is also relevant to individuals' access to and control over data about themselves. It provides as follows:

1. *Everyone shall have the right to hold opinions without interference.*
2. *Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
3. *The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
    a. *For respect of the rights or reputations of others;*

[12] David Banisar, 'Privacy and Human Rights: An International Survey of Privacy Laws and Practice', available at: http://gilc.org/privacy/survey/intro.html.

[13] Australian Law Reform Commission, (2008) 'For Your Information: Australian Privacy Law and Practice (ALRC Report 108), page 148, available at: https://www.alrc.gov.au/publications/report-108.

[14] Australian Law Reform Commission, (2008) 'For Your Information: Australian Privacy Law and Practice (ALRC Report 108), page 153, available at: https://www.alrc.gov.au/publications/report-108.

b. *For the protection of national security or of public order, or of public health or morals.*

Article 19.2 recognises individuals' freedom to seek, receive and impart personal data through any media of their choice. This human right is not prescriptive of the types of data, classes of recipient or the purpose of the communication to which it purports to apply.

The right to privacy and Australian privacy law

In Australia, information privacy is primarily protected by the Privacy Act, which establishes an express or implied consent model.[15] The Privacy Act contains the Australian Privacy Principles (APPs), which apply to government agencies and private organisations. Most small businesses with an annual turnover of less than $3 million are exempt from the Privacy Act, though this is not the case for small businesses that are:

- reporting entities for the purposes of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and associated regulations;
- ballot agents for the purpose of the *Fair Work Act 2009* (Cth);
- small businesses that are an association of employees registered or recognised under the *Fair Work (Registered Organisations) Act 2009* (Cth); and
- any small business prescribed in accordance with regulations made under the Privacy Act or carrying out acts or practices prescribed by regulations under the Privacy Act.

This is not an exhaustive list of small businesses who are not exempt from the Privacy Act.[16]

A number of other exemptions to the Privacy Act also apply, including for employee records, individuals who are acting in a non-business capacity, journalism, and political acts and practices.

---

[15] NB: Collection, use and disclosure may be permitted without actual consent (express or implied) where it is reasonably necessary or expected for the performance of a business's functions. It may also be permitted in other cases, such as when otherwise authorised by law.

[16] see subsection 6D(4) of the Privacy Act, available at: https://www.legislation.gov.au/Details/C2018C00456.

The APPs outline how APP entities must handle, use and manage personal information. Entities regulated by the Privacy Act must take such steps as are reasonable in the circumstances to notify individuals of factors including the purposes for collecting the information, who the organisation usually discloses information of that kind to, and whether the personal information is likely to be disclosed overseas. The APPs also cover maintaining quality and security of personal information and rights for individuals to access and correct their personal information. They place more stringent obligations on APP entities when they handle sensitive information. A summary of the APPs and how they compare to the CDR privacy safeguards can be found in Appendix A.

The Privacy Act contains a number of possible enforcement mechanisms. This includes a breach notification scheme for serious breaches of APP 11, and the ability for individuals to complain about a breach of the Privacy Act to the OAIC. The OAIC then assesses whether it can investigate the complaint. The Information Commissioner must take reasonable steps to conciliate complaints, but may decide not to investigate the complaint further. The OAIC is also able to undertake Commissioner-initiated investigations and accept enforceable undertakings. In recent times, it has been provided with the power to seek civil penalties for serious and repeated interferences with privacy, but it has not yet sought a civil penalty under the Privacy Act.

PIA Methodology

Privacy Impact Assessment process

This PIA was prepared in accordance with the Code and the OAIC PIA Guidance.[17]

The Code requires Australian Government agencies to conduct a PIA for all high privacy risk projects, which may include where a project involves any new or changed ways of handling personal information that are likely to significantly impact the privacy of individuals.

[17] Office of the Australian Information Commissioner, (2014) 'Guide to undertaking privacy impact assessment' (OAIC PIA Guidance), available at: https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf.

Privacy Impact

Treasury considers that the CDR has a significant privacy impact, and that it is appropriate to conduct a PIA for the CDR, for the following reasons:

- It allows easier transfer of specified data, which will include personal information.
  - As the CDR is intended to be an economy-wide right, it will affect and involve many types of personal information
- It will create new Privacy Safeguards that will affect the way CDR participants handle, store and transfer personal information.
- The CDR involves threats to privacy at each stage of the data transfer.

Treasury has determined that the PIA should include a detailed analysis of the threats and mitigation strategies, in order to better manage these threats during implementation of the CDR.

Conduct of the PIA

This PIA has been developed by Treasury drawing upon extensive ongoing consultation with relevant stakeholders on privacy threats and proposals as part of the broader development of the regime.

The OAIC PIA Guidance provides that:

> "Generally, whoever is managing the project would be responsible for ensuring the PIA is carried out. The nature and size of the project will influence the size of the team needed to conduct the PIA, and how much the team needs to draw on external specialist knowledge.
>
> A PIA is unlikely to be effective if it is done by a staff member working in isolation. There could be a team approach to conducting a PIA, making use of the various 'in-house' experts available, such as the privacy officer or equivalent, and outside expertise as necessary. A range of expertise may be required, including information security, technology, risk management, law, ethics, operational procedures and industry-specific knowledge. Seeking external input from experts not involved in the project can help to identify privacy impacts not previously recognised.

> Some projects will have substantially more privacy impact than others. A robust and independent PIA conducted by external assessors may be preferable in those instances. This independent assessment may also help the organisation to develop community trust in the PIA findings and the project's intent.
>
> The team conducting the PIA needs to be familiar with the Privacy Act, any other legislation or regulations that might apply to personal information handling (for example, state or territory legislation), and the broader dimensions of privacy." [18]

A decision was made not to outsource the development of the PIA to external consultants. This has been criticised by some stakeholders.

The CDR regime as a whole is largely directed at protecting the data of consumers, including individuals' data. It was therefore not appropriate to separate the assessment of privacy impacts and proposals to address privacy threats from the core policy development function being undertaken by Treasury.

This development process took place over approximately 18 months, in an iterative way, involving multiple consultations. This did not lend itself to a point in time assessment by external consultants.

The internal development of the PIA also reflects Treasury's recognition of the importance of developing internal capability in relation to PIAs and a better understanding of the privacy issues and risks raised by the CDR as part of its design. This was a secondary factor in the decision to conduct the PIA internally and had little influence on the decision.

Initial shortfalls in Treasury's capabilities to develop a PIA were addressed through staff development, internal research and engagement with privacy experts over the course of the process.

The Government has committed to a post-implementation review of the CDR. The requirement for this review (and that it must be independently conducted) will be mandated

[18] OAIC PIA Guidance, page 10.

by legislation.[19] The findings of this independent review will be required to be tabled before the Australian Parliament.

The PIA process is iterative, particularly as this PIA has been prepared at a reasonably early stage of implementation of the CDR. Further PIAs will be required as the CDR is expanded and developed (see 'next steps' below).

Consultation

The privacy aspects of the CDR have been the subject of extensive consultation.

In accordance with the OAIC PIA Guidance, consultations have previously taken place on the privacy threats and concerns associated with introducing consumer data access and portability rights and options to mitigate those threats, as part of:

- the PC Report;
- the Taskforce established to consider the Government's response to that Inquiry;
- the OBR;
- the Government's consultation on the Final Report of the Open Banking Review;
- consultations on two drafts of the Treasury Laws Amendment (Consumer Data Right) Bill 2018;
- consultations by the ACCC on its proposed Consumer Data Right rules framework; and
- consultations by the interim Chair of the proposed Data Standards Body on proposed technical standards.

As part of those consultations, a broad range of stakeholders have made formal and informal written submissions and oral submissions (such as at roundtables or bilateral meetings), and opportunity has been provided to stakeholders to gain a better understanding of, and provide comment on, any proposed mitigation strategies.[20]

[19] See clause 56GH of the Treasury Laws Amendment (Consumer Data Right) Bill 2019, which provides that this review must report by 1 January 2022.

[20] OAIC PIA guidance, page 11.

The assessment has also benefited from public commentary on the proposed reforms and from observations of the implementation of Open Banking in the United Kingdom.

Further detail of consultations forming part of this privacy assessment is set out in the Stakeholder Consultation section of this PIA.

Additionally, the first version of the PIA was subject to public consultation between 21 December 2018 and 18 January 2019. This second version of the PIA incorporates feedback from the 15 submissions received as part of that process. The first version of the PIA was also subject to limited targeted consultation between 20 November and 30 November 2018.

The OAIC PIA Guidance provides the following requirements for consultation, which have been met in relation to the proposed reform: [21]

> "Consulting with stakeholders may assist in identifying privacy risks and concerns that have not been identified by the team undertaking the PIA, and possible strategies to mitigate these risks. Consultation may also offer stakeholders the opportunity to discuss risks and concerns with the entity and to gain a better understanding of, and provide comment on, any proposed mitigation strategies. Importantly, consultation is also likely to provide confidence to the public that their privacy has been considered. Failure to consult may give rise to criticism about a lack of consultation in relation to the project.
>
> For consultation to be effective, stakeholders will need to be sufficiently informed about the project, be provided with the opportunity to provide their perspectives and raise any concerns, and have confidence that their perspectives will be taken into account in the design of the project. Many consultation models are available, including telephone or online surveys, focus groups and workshops, seeking public submissions, and stakeholder interviews. Different models will be appropriate for different stakeholder groups and different stages of the project, and careful consideration should be given to which consultation model/s will be appropriate in the circumstances.

[21] OAIC PIA guidance, page 11.

Consultation does not necessarily need to be a separate step as it can be useful to consult throughout the PIA process. It is important that some form of targeted consultation is undertaken, even if widespread public consultation is not possible (for example, if a private organisation is concerned about sharing commercially sensitive information widely), such as with groups representing relevant sectors of the population, or advocacy groups with expertise in privacy."

Next steps

This second PIA has been developed based on the proposed legislative framework for the CDR, recent key design decisions on the Rules and Standards, and consultation on the first version of the PIA.

The ACCC released its Rules Framework paper for consultation on 11 September 2018 to 12 November 2018, receiving 54 submissions. A decision paper on the draft Rules was released in December 2018.

Data61 is developing technical standards with the benefit of advice from an Advisory Committee which includes industry, FinTech, privacy and consumer representatives. Three industry working groups have been established that are open to all interested parties, on: APIs Standards; Information Security; and User Experience. The standards are being developed transparently and iteratively through GitHub. Collated draft standards were released for consultation from 2 November 2018 until 23 November 2018. A subsequent draft was released in December 2018. Additional standards on matters such as information security are being developed in parallel.

Ongoing development work, including from the Government's commitment to informing the design of the system through consumer testing, will mean that not all detail of the regime will be settled before the Bill is introduced. A new or updated PIA will need to be prepared once all design features are settled, after testing has identified any consumer and privacy threats, and prior to the launch of access to consumer data in February 2020.

Where new sectors are designated or the Rules amended, the legislation requires the ACCC and Minister to consider the privacy impacts. Where such changes significantly impact privacy, the ACCC may review the PIA or undertake a fresh PIA. New PIAs will be developed

as part of any future sectoral assessments, prior to a sector being designated as being subject to the CDR.

Stakeholder Consultation

Consultation during the Productivity Commission's Inquiry into Data Availability and Use

In May 2017, the Government received the PC Report which included a set of 41 recommendations, including for the creation of a new economy-wide Comprehensive Data Right. In developing these recommendations, the PC conducted extensive stakeholder consultation.

On 18 April 2016, the PC released an Issues Paper seeking comments from interested parties until 29 July 2016.[22] The PC received 211 public submissions during this period, which have been made available on the Inquiry website.[23] The Issues paper included a section concerning individuals' access to and control over data about them. This followed on from a recommendation in the 2015 Competition Policy Review (mentioned above) that supported allowing consumers to access information in an efficient format.

On 3 November 2016, the PC released its Draft Report for public comment with consultation open until 12 December 2016.[24] The report included a draft recommendation for a new Comprehensive Right for individuals. The PC received 125 public submissions in response to the Draft Report.

Submissions to the Inquiry included: 94 from industry associations or representative bodies; 69 from governments or government agencies; 59 from private sector businesses; 58 from academics or research groups; 38 from individuals; and 18 from not-for-profit or other non-business groups.

---

[22] Available at: https://www.pc.gov.au/inquiries/completed/data-access/issues/data-access-issues.pdf.

[23] Available at: https://www.pc.gov.au/inquiries/completed/data-access/submissions.

[24] Available at: https://www.pc.gov.au/inquiries/completed/data-access/thedraft/data-access-draft.pdf.

All public submissions have been made available on the Inquiry website.[25] In addition, the PC held separate discussions with around 130 businesses, business groups, academics, government agencies and individuals in Australia and overseas. Three roundtable discussions were held during the Inquiry — with academics; with Australian Government agencies; and with members of the Business Council of Australia. Public hearings were held in Melbourne on 21 November 2016 and in Sydney on 28 November 2016.

On 8 May 2017, the Government released the PC's Final Report for the Inquiry.[26] As outlined above, the Report included 5 recommendations on a new Comprehensive Right for consumers.

Consultation during the Government's Data Availability and Use Taskforce

The Government's Data Availability and Use Taskforce (Taskforce) developed a Government response to the PC's Data Availability and Use Inquiry. In its Response, the Government agreed to 33 of the Inquiry's 41 recommendations including the implementation of the new CDR which was to be informed by the findings of the Open Banking Review.

In developing the Government's response, the Taskforce consulted with 83 interested parties including Commonwealth agencies, States and Territories, and other significant stakeholders. Consulted parties included: 78 peak industry bodies and businesses, including the banking, telecommunications and energy sectors; 15 community, consumer and society representatives; 16 research sector bodies; 43 Commonwealth public sector bodies; and 9 State and territory public sector bodies.

As a result of stakeholder feedback, the CDR proposed by the Government's Taskforce varied from the model proposed in the PC Inquiry, but maintains some similarities to the PC's proposed comprehensive data right.

[25] Available at: https://www.pc.gov.au/inquiries/completed/data-access/submissions.

[26] Available at: https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf.

Departures from the PC's proposed economy-wide-by-default approach that are relevant to this PIA include:

- The CDR will be progressively rolled out on a sector-by-sector basis beginning in the banking, energy and telecommunications sectors. As the right will not immediately apply comprehensively across the economy, it was considered more appropriate that it be labelled the Consumer Data Right. The roll-out to additional sectors will involve cost benefit analysis including in relation to privacy impacts.
- The CDR will explicitly recognise the dual nature of an individual's personal information, in the sense that it holds both fundamental human rights aspects and an economic character.
  - The CDR regulatory model will ensure that competition, consumer and privacy outcomes are balanced.
  - Future sectors to be designated will be determined by the Treasurer in consultation with the ACCC and the OAIC.
  - The ACCC will be the primary regulator responsible for competition and consumer matters, including setting the Rules and Standards, with the OAIC being primarily responsible for privacy matters and complaints handling (though note that between the regulators, there will be a 'no wrong door' approach to consumer complaints). This moves away from the PC's proposal to have the ACCC as the single regulator.

Consultation during the Open Banking Review

The OBR consulted with over 100 stakeholders to consider issues in the current data sharing environment.

On 9 August 2017, the OBR released an Issues Paper seeking comment from interested parties for a period of six weeks.[27] The Issues Paper called specifically for advice on how data should be shared under open banking, and on ways to ensure that privacy is protected and

[27] The Treasury (2017), 'Review into Open Banking in Australia – Issues Paper', available at: https://static.treasury.gov.au/uploads/sites/1/2017/08/Review-into-Open-Banking-IP.pdf.

shared data is kept secure. Comments received were used to inform the Review's chapters on privacy safeguards and the data transfer mechanism.

The OBR received 39 non-confidential submissions (available on the OBR's website) and one confidential submission.[28] The OBR conducted two public roundtable consultations in Sydney and Melbourne, and one roundtable dedicated to privacy issues with privacy and consumer advocates and academics in Canberra. In addition, the OBR held over 100 meetings with interested parties such as banks, FinTech firms, consumer advocates and regulators.

Stakeholders raised a range of privacy concerns. These issues were generally broad privacy policy concerns related to the introduction of the CDR, but submissions sometimes addressed matters outside of the CDR's scope.

Some submissions advocated for stronger privacy protections than those currently available under the Privacy Act, arguing that they are inadequate compared to those in other countries. However, many supported the extension of existing privacy frameworks to the CDR. Some submissions advocated for protections similar to those under the European Payment Services Directive 2 (PSD2) and the GDPR including meaningful, unbundled and informed consent, behaviourally tested consent disclosures and data erasure and portability rights. Some stakeholders also argued that the Privacy Act should be extended to include small to medium enterprises. Overall, submissions called for a cohesive fit-for-purpose regulatory framework with well-resourced, proactive regulators.

Submissions cautioned against a range of threats involved with data sharing. These included the threat of further eroding trust in the banking system in cases of breaches or data misuse. Additionally, there were concerns that increased complexity and choice from new products could lead to sub-optimal consumer choices, and that there could be a reduction in positive friction in decision making. There were also concerns that there could be an increase in predatory practices likely to cause increased economic inequality, such as risk segmentation, profiling for profit, price discrimination, digital exclusion, use of non-transparent terms and conditions, black box technology and biased algorithms which lead to poor consumer outcomes.

[28] Available at: https://treasury.gov.au/consultation/review-into-open-banking-in-australia/.

Consultation following the Open Banking Review

On 9 February 2018, the Government released the Report from the OBR for public comment for a period of six weeks, in order to assist with developing details for implementation.[29] Privacy was a key consideration during the OBR. The Final Report included a chapter which outlined privacy concerns and the proposed Privacy Safeguards, to ensure that the risks identified by privacy and consumer advocates were addressed and considered. The chapter included detailed recommendations about divergence from the Privacy Act, appropriate consent requirements, the issue of a right to deletion, and a comprehensive liability and dispute resolution framework.

The consultation received 74 submissions, with 7 submissions being confidential. Non-confidential submissions have been made available on the OBR's website.[30] Some submissions raised concerns about a lack of transparency and genuine individual consent to use of data when signing up for products and services. Additionally, some submissions called for review and modernisation of the Privacy Act and the APPs to increase protections for individuals participating in the CDR. The privacy concerns raised are listed in more detail in Appendix B. It should be noted that some of these are questions of broader privacy policy, beyond the scope of the CDR.

Consultation on the Treasury Laws Amendment (Consumer Data Right) Bill 2018

On 15 August 2018, the Government released an Exposure Draft of the Treasury Laws Amendment (Consumer Data Right) Bill 2018, which will amend the *Competition and Consumer Act 2010 (Cth)* to establish the CDR Framework.[31] The initial round of consultation was open until 7 September 2018. The consultation received 65 submissions from a range of stakeholders, including community representatives.

---

[29] The Treasury (2018), 'Review into Open Banking in Australia – Final Report', available at: https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

[30] Available at: https://treasury.gov.au/consultation/c2018-t247313/.

[31] Available at: https://treasury.gov.au/consultation/c2018-t316972/.

Treasury undertook a second round of consultation on the Exposure Draft Bill between 24 September 2018 and 12 October 2018, receiving 25 submissions.[32]

Treasury conducted eight stakeholder roundtables between 23 and 31 August 2018 – three in Sydney, three in Melbourne, one in Canberra, and one with academics and consumer advocates across Australia via teleconference. In total, approximately 150 people attended these roundtables and were asked to provide input to this PIA as part of their submissions.

Treasury has also conducted bilateral meetings with privacy academics and advocates since February 2018 and will continue to do so.

A number of stakeholders engaged with the privacy aspects of the Exposure Draft Bill. Many stakeholders welcomed the introduction of the Privacy Safeguards, noting that they would provide stronger privacy protections than the APPs, although some stakeholders felt that the Safeguards should be strengthened. Other privacy related concerns included:

- that the introduction of Privacy Safeguards creates unnecessary complexity, both for individuals to navigate their rights under separate regimes and from a compliance perspective for participants;
- requests for clarification on the interaction between the Privacy Act and the Privacy Safeguards, including as to when each of these regimes apply and whether an entity's CDR privacy policy could be merged with its existing APP privacy policy;
- requests for simplification of the CDR privacy regime;
- that only the APPs should apply to the CDR, either in their existing form or strengthened in line with the GDPR;
- that the Privacy Safeguards should be more detailed, for example in relation to the definition of valid consent, rather than leaving this detail to the Rules;
- that all Privacy Safeguards should apply to data holders and to all CDR data;
- that foreign CDR participants should be subject to the Privacy Act;
- that there should be a broad right to deletion;

[32] Available at: https://treasury.gov.au/consultation/c2018-t329327/.

- that on-sale of personal data should be banned; and
- concerns about the significance of penalties applying to breaches of the Privacy Safeguards and views that only serious or repeated breaches of the Privacy Safeguards should be penalised.

Some concerns were also raised regarding the process for preparing the PIA – in particular, that it should be prepared independently.

Consultations on the Consumer Data Right Rules and Standards

Consultations are ongoing in relation to the ACCC's development of the Rules; and the development of the consumer data right technical standards by the interim Data Standards Body (the Data61 branch of the CSIRO).

The ACCC released its Rules Framework paper for consultation from 11 September 2018 to 12 November 2018, receiving 54 submissions.[33] The ACCC released a Rules outline paper, setting out the ACCC's position in relation to the first version of the Rules, on 21 December 2018. The Rules are expected to be published for consultation in the first quarter of 2019.

Data61 is developing technical standards with the benefit of advice from an Advisory Committee which includes industry, FinTech, privacy and consumer representatives. Three industry working groups have been established that are open to all interested parties: on APIs Standards; Information Security; and User Experience. The standards are being developed transparently and iteratively through GitHub. Collated draft standards were released for consultation from 2 November 2018 until 23 November 2018. A subsequent draft was released in late December 2018, for consultation until 18 January 2018. Additional standards on matters such as information security are being developed in parallel.

[33] Available at: https://www.accc.gov.au/focus-areas/consumer-data-right/accc-consultation-on-rules-framework.

Consultation on version 1 of the Privacy Impact Assessment

The Government consulted on the text of version 1 of the PIA between 21 December 2018 and 18 January 2019. 15 submissions were received. Treasury also undertook limited consultation on the text with privacy stakeholders between 20 November and 30 November 2018, and consulted with the ACCC and the OAIC on drafts of the PIA.

Key concerns raised by stakeholders related to the process for development of the PIA, calls for undertaking reform to Australia's broader privacy framework before implementing the CDR and/or strengthening privacy protections in the CDR framework, that some threats should be assessed as having a higher likelihood of occurrence or higher severity, that there should be further consumer testing, and that there should be further consideration of impacts on vulnerable consumers.

Stakeholders also raised a number of issues for consideration by the ACCC and Data61 in relation to the Rules and Standards respectively, for example, conditions for accreditation of data recipients.

This second version of the PIA incorporates feedback received during these consultations.

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 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).

It should be noted that Naomi is also able to direct her current credit card provider to directly provide her with her own data, so that she can engage a comparison website directly.

Stage 2: Individual authorises use and collection of data

BetterDeals offers Naomi the option of tailored advice if she consents to it collecting and using her credit card data for that purpose.

In this same stage, Naomi consents to the collection and use of her data by BetterDeals for those specific purposes.

Stage 3: Individual consents to disclosure

BetterDeals refers Naomi to her bank, National Nickle Bank (NN Bank, the data holder), so that she can provide them with her consent to disclose that information.[34] As part of the consent process, NN Bank authenticates her identity.

NN Bank will need to ensure that the consent to disclosure accords with the consent requirements in the Rules, and check the Accreditation Register to ensure that BetterDeals is an accredited data recipient.

Stage 4: Data holder discloses to the data recipient

Having received Naomi's consent, NN Bank then discloses her credit card data to BetterDeals.

Stage 5: Data recipient receives data and uses data

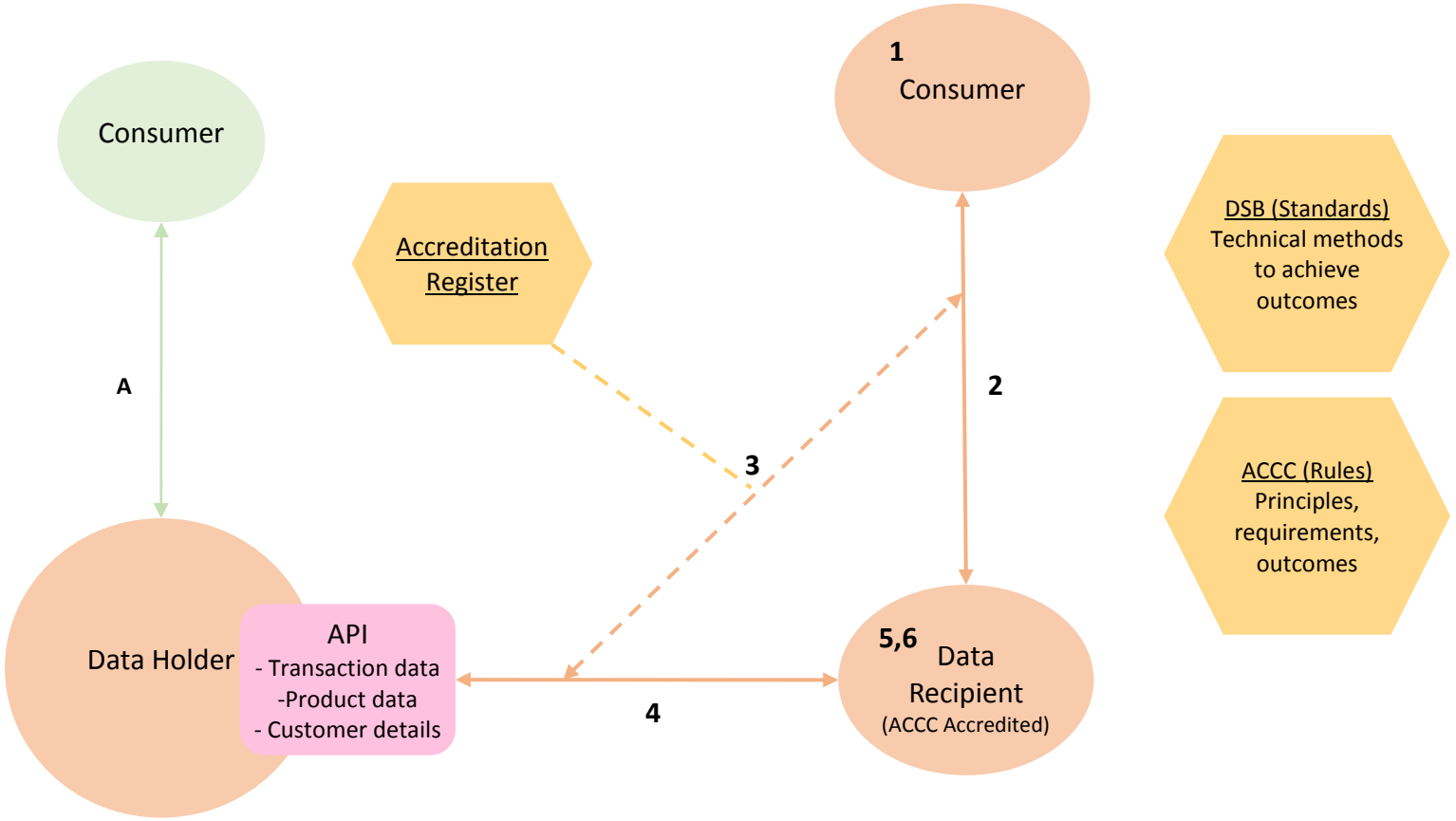
This data is received by BetterDeals who analyses Naomi's data together with data on all of the credit card products that are available to recommend the credit card account which would best suit Naomi's usage and personal circumstances.

[34] There are three authentication models that could be used to refer an individual to their bank to provide their consent to disclose data: a decoupled approach; a redirect approach; or a known channel redirect approach. The Data Standards Body is developing standards that will detail the proposed methods of authentication. Further detail is in the 'phishing' section below.

Stage 6: Deletion or de-identification

Having used the data for all the purposes consented to by Naomi, BetterDeals destroys or de-identifies her data.

Consumer Data Right Framework Simple Information Flows



Stage 1: Individual engages with data recipient
Stage 2: Individual authorises use and collection of data
Stage 3: Individual consents to disclosure
Stage 4: Data holder discloses to the data recipient
Stage 5: Data recipient receives data
Stage 6: Deletion

Stage A: Consumer may obtain data directly from data holder

Key:
ACCC – Australian Competition and Consumer Commission
API – Application Programming Interface
DSB – Data Standards Body

Additional Consumer Data Right scenarios

There are several possible ways for the information to flow through other parties:

(a) Naomi may access BetterDeals' services through an **intermediary** such as a financial advisor, or a social media or other digital platform. If the intermediary is not accredited, this could only occur where permitted by the Rules.

(b) Rather than developing their own API (the channel through which data is provided), NN Bank may outsource to a third party who will **provide an API** on their behalf.

(c) Similarly, BetterDeals may outsource some of its functions to a third party to, for example, **store data on a cloud service** or process and analyse the data.

(d) BetterDeals may engage the services of an accredited intermediary to connect to NN Bank. An intermediary may be a contractor/agent for BetterDeals or may be a separate data recipient in their own right. This intermediary might also provide services to BetterDeals, such as **filtering or processing transaction data** from the data holder. An intermediary may also be a designated gateway (a sub-class of intermediary), as defined in the Bill. BetterDeals may be required to transfer data through a designated gateway. Designated gateways will only be able to collect, use and disclose information as specifically provided for in the Rules.[35]

(e) Naomi may also request BetterDeals to transfer her data to another accredited party, such as a **budgeting application**.

(f) Naomi may also request BetterDeals to transfer Naomi's data to a **non-accredited party** such as her accountant, thus the data would leave the CDR system (if this is permitted by the Rules).

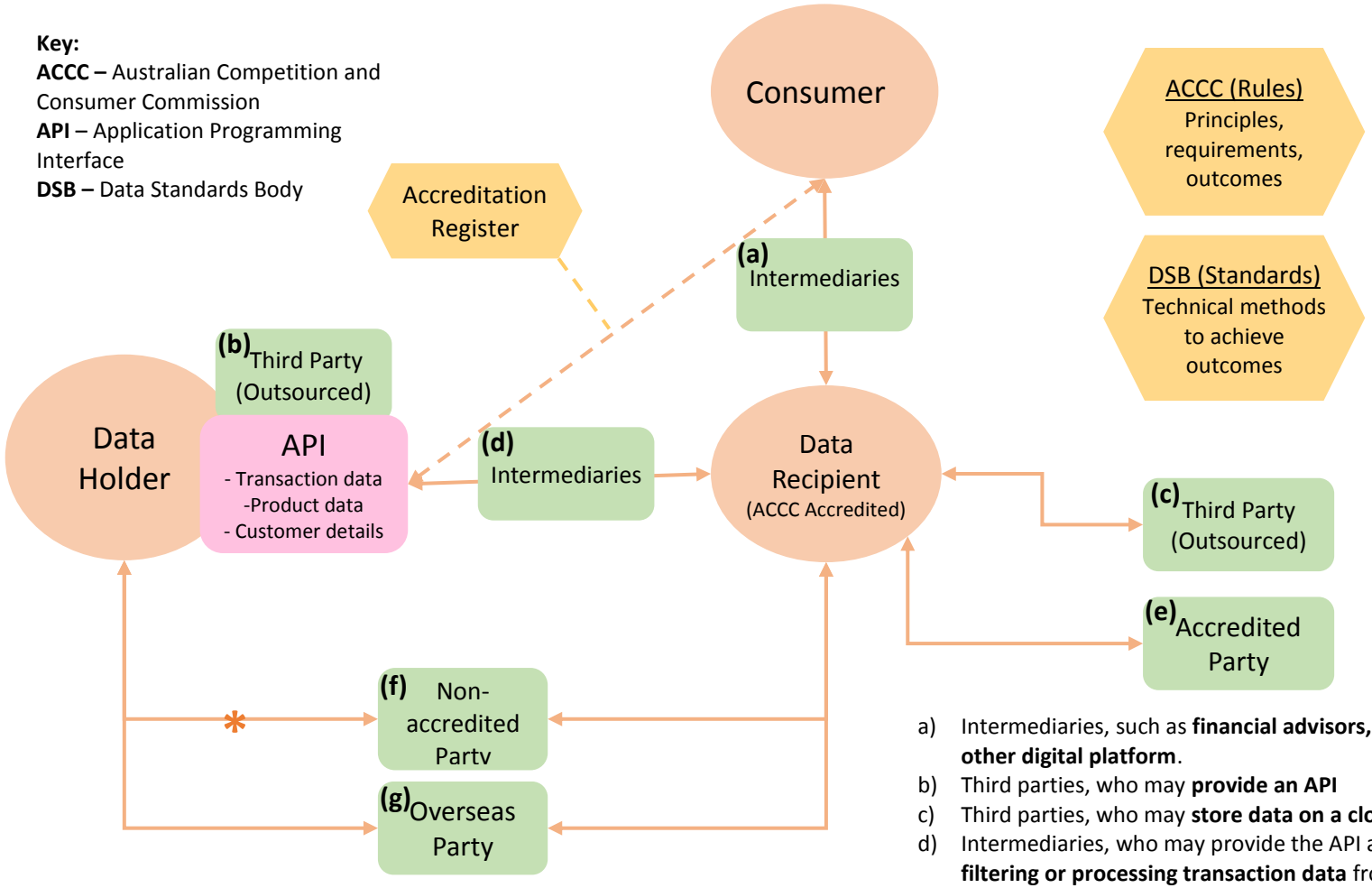
(g) Finally, Naomi may want to transfer her data to an **overseas recipient**.

e.g. Naomi is moving to New Zealand and requests that BetterDeals transfers her data to their New Zealand affiliate to help her select a card from a New Zealand bank.

[35] References to an intermediary in this document should be read as including designated gateways.

Consumer Data Right Framework Complex Information Flows

Key:
ACCC – Australian Competition and Consumer Commission
API – Application Programming Interface
DSB – Data Standards Body



a) Intermediaries, such as **financial advisors, or a social media or other digital platform**.
b) Third parties, who may **provide an API**
c) Third parties, who may **store data on a cloud service**
d) Intermediaries, who may provide the API and services such as **filtering or processing transaction data** from the data holder
e) Other accredited parties, such as a **budgeting applications**
f) **Non-accredited parties**
g) **Overseas recipients**

*Within the CDR this information flow would only be of information for which there is not an identifiable consumer, such as product information.

Note: like the simple diagram, direct to consumer is also possible here.

Designated Gateways

The legislation allows for the Minister to designate a gateway for some sectors to facilitate the transfer of information from the data holders to data recipients or the consumer themselves.

The rules may mandate the use of designated gateways for accessing information if one has been designated.

Designated gateways might be used where the gateway entity already has a role in gathering and disseminating the data, and where use of existing legal frameworks and infrastructure may contribute to improved efficiency, safety or consumer convenience.

The Government has indicated that it expects gateways would ordinarily be Commonwealth bodies or entities, but no gateways have yet been designated for any sectors. Should any gateways be designated in the future, future PIAs will need to address them in more detail.

Impacts on Privacy

The transfer of an individual's personal data from data holder to data recipient involves multiple stages as outlined in the 'Mapping of Personal Information' section above. The following section identifies and critically analyses the potential privacy threats and their likely consequences at each stage of the data transfer.

Threats outlined in this section are categorised as one of six types in relation to the point in the process at which the threat could occur (according to the type of threat they most closely relate to). A threat may be a(n):

- **Identification Threat** – meaning a threat to privacy arising from the misidentification of a consumer, data holder or recipient, whether through inadvertence or misleading conduct.
- **Authorisation Threat** – meaning a threat arising during the process of the customer consenting to collection, use or disclosure of the personal data. This includes threats as to whether authorisation is genuine and whether authorisations are complied with.
- **Transfer Threat** – meaning a threat to privacy arising during the communication of information from one party to another. This may involve transfers such as the

communication of information regarding the data transfer, the data transfer itself, or any other incidental information transfers.

- **Holding Threat** – meaning a threat to privacy arising from a failure to secure data against improper disclosure or use, either by internal or external actors.
- **Usage Threat** – meaning a threat to privacy arising from use of the data by the parties who obtain customer data, either through negligence or misconduct.
- **Data Quality Threat** – meaning a threat to privacy arising from inaccurate, misleading or incomplete information being collected, used or disclosed.

The threats identified in this section are mainly focussed on privacy, however, not mentioned in this assessment are other threats that may exist. This includes the potential negative impact of the CDR on some consumer outcomes, on the stability and efficiency of markets, and social impacts (such as due to increased or new forms of differentiation in price, quality and availability of goods and services to different classes of individual). These have been considered as part of the policy development process, but are not documented in this PIA.

The table below also notes that most of the privacy threats exist in relation to current data sharing practices, which, as outlined above, are often unregulated. While the CDR may exacerbate or adjust the nature of some of these threats, the privacy protections provided in the CDR system will mitigate these threats.

It should be noted that in addition to the threats to the privacy of the individual, each of these scenarios would also pose a reputational threat to the CDR system itself.

Threats also exist in relation to the effectiveness of the governance and operation of the regulatory framework.

Risk Assessment

The threats identified in this section have been assessed according to a modified form of the Treasury's risk rating matrix. The risk assessment framework takes into account the likelihood of each threat occurring and the severity of their potential consequences to determine a risk rating between "Very Low" and "Severe". The likelihood and consequence descriptions in Treasury's risk rating matrix were modified to be more relevant to the CDR.

Risk Rating Matrix

This PIA applies the risk rating matrix below to categorise each of the threats identified in the next section. For example, Treasury considers that a situation that occurs rarely with a major consequence would have a "Low" rating.

Table 4: Modified form of Treasury's risk rating matrix

		Consequence				
		Insignificant	Minor	Moderate	Major	Extreme
Likelihood	Almost Certain	Low	Medium	High	Severe	Severe
	Likely	Low	Low	Medium	High	Severe
	Possible	Low	Low	Medium	Medium	High
	Unlikely	Very Low	Low	Low	Medium	High
	Rare	Very Low	Very Low	Low	Low	Medium

Table 5 below provides guidance for determining the likelihood and consequence ratings for the privacy impacts identified in the CDR. The risk ratings are applied to the identified threats to determine the overall rating.

Treasury conducted a series of internal workshops in order to determine an appropriate assessment of the likelihood and severity of each privacy threats. Treasury staff trained in Structured Analytic Techniques (SATs) led the workshops to systematically incorporate the independent views of the project team into a combined assessment. Treasury used SATs such as a structured brainstorm and horizon scanning to apply different perspectives and ways of thinking to the problem, and reduce the possibility of groupthink.

Table 5: Likelihood and consequence ratings for the privacy impacts identified in the CDR

Rating	Likelihood Description
Almost Certain	The threat to the individual/business is almost certain to eventuate within the CDR system.

Rating	Consequence Description
Extreme	The threat to the individual/business results in severe reputational damage, severe emotional or physical harm, and/or

			extreme financial loss.
Likely	The threat to the individual/business will probably eventuate within the CDR system	**Major**	The threat to the individual/business results in significant reputational damage, significant emotional or physical harm, and/or significant financial loss.
Possible	The threat to the individual/business may eventuate within the CDR system	**Moderate**	The threat to the individual/business results in reputational damage, emotional or physical harm, and/or financial loss.
Unlikely	The threat to the individual/business may eventuate within the CDR system at some time but is not likely to occur	**Minor**	The threat to the individual/business results in minor reputational damage, minor emotional or physical harm, and/or minor financial loss.
Rare	The threat to the individual/business will only eventuate in exceptional circumstances or as a result of a combination of unusual events	**Insignificant**	The threat to the individual/business results in insignificant: reputational damage; emotional or physical harm; and/or financial loss.

The likelihood of threats arising was assessed with regard to an individual participating in the CDR over a given year and across multiple interactions with multiple data recipients and data holders.

> e.g. Over a given year a consumer exercising their rights under the CDR in respect of multiple data holders is *unlikely* to suffer loss from threat X, but where they do the consequences are most likely to be *major*.

The likelihood assessment **does not** reflect the probability of harm per interaction with the system. Adopting such an approach generally resulted in a 'rare' assessment against each threat and therefore did not provide meaningful information to a reader seeking to assess the level of a given privacy threats.

The likelihood of each threat occurring was also not assessed across the individual's lifetime exposure to the CDR.

A decision was taken not to assess threats at the group level, as in many cases this would increase the likelihood and/or severity attached to those threats in a way that would not provide meaningful information to a reader seeking assess the level of a given privacy threat.

Similarly, the risk assessments **do not** take into account reputational damage to the CDR system itself. This was considered outside the scope of this PIA which focusses on harm to individuals.

The privacy impacts table and analysis in this section **does not** take into account any of the risk mitigation strategies in the CDR framework.

For example, in the absence of any protections, the threat of a malicious third party seeking to mislead a data holder that they are a particular data recipient in order to obtain data has a moderate likelihood with potentially severe consequences. However, the proposed information security arrangements (such as digital certificates, accreditation registers with real time look up and encrypted communications) are expected to reduce this likelihood to 'rare'. See Tables 7 and 8 below for an assessment of the likelihood of these threats occurring once mitigation strategies are applied.

The analysis in this section **does** takes into account pre-existing risk mitigation arrangements – including existing laws (such as the Privacy Act), practices and system (such as cyber security arrangements), and behaviours (such as individuals generally exercising caution and due care when dealing with transferring personal data). This includes arrangements that are already in place to mitigate both the likelihood and consequences of some threats.

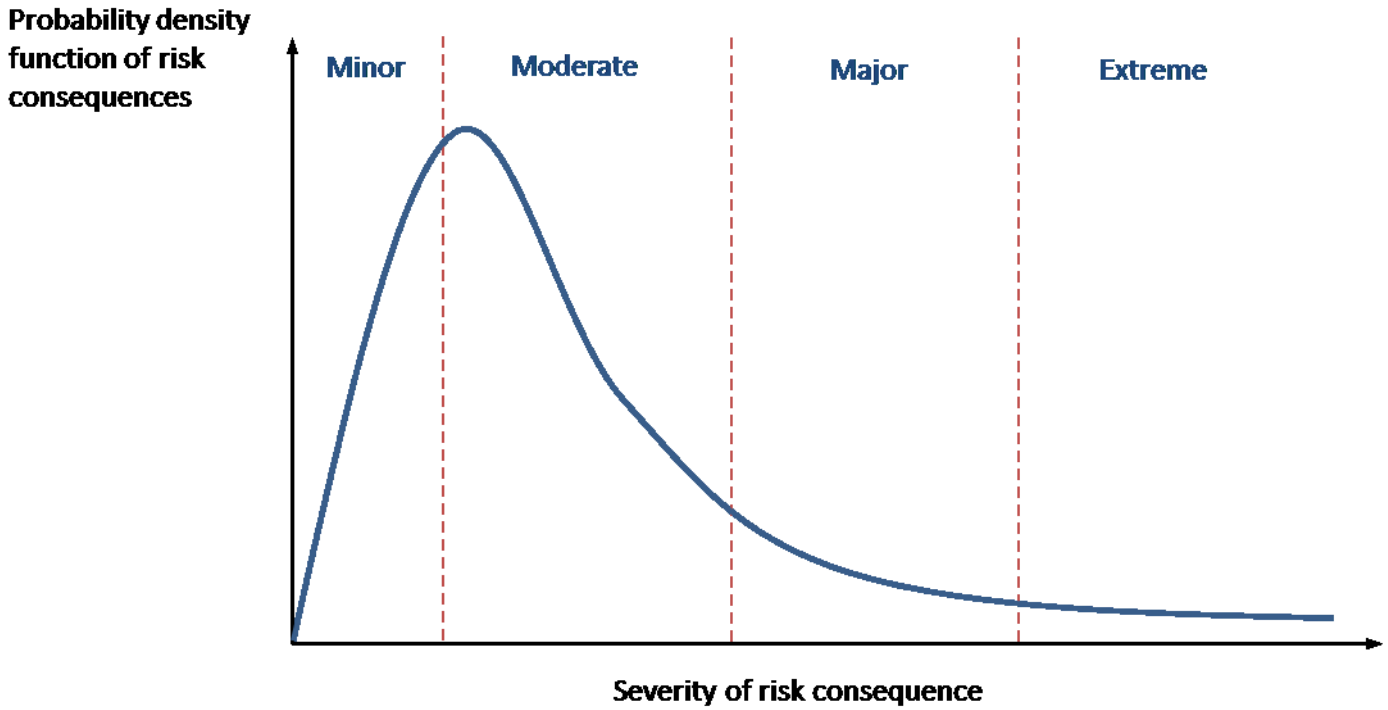
The assessment of the potential severity of the consequences of a privacy threat being realised has sought to take into account harm arising from:

- the infringement on the individual's fundamental human right to privacy;
- any financial loss;
- personal and psychological harm;
- emotional harm falling short of psychological harm, including arising from a feeling of violation or from suffering inconvenience; and
- consequential loss, such as rectification costs.

The severity of the consequence of the identified threat will vary based on any given situation. A given threat identified in the CDR may not result in any meaningful financial, emotional, physical or reputational loss or harm to the individual or business in all cases.

Therefore, when assessing each threat, it is appropriate to consider that severity will generally follow a probability distribution rather than a discrete categorisation of severity (which might otherwise be implied in the risk rating framework).

Figure 1: Distribution of severity for realised risks



The diagram above shows that each threat has varying degrees of severity, depending on the individual's unique situation.

In the example case drawn out in Figure 1, it can be seen that most of cases fall within the 'Moderate' portion of the probability function (that is, the area under the curve is largest for this region). Therefore, we would rate the severity of the consequence in this case to be "Moderate".

However, the distribution's long tail implies that there are some cases in which an extreme consequence, for example identity theft or fraud, could be envisioned for this particular threat.

An example to help illustrate this point is a situation in which a data breach contributes to identity theft which enables funds to be stolen from an individual's account. Individuals with higher account balances will have a greater possibility of losing higher amounts of money, making the consequence more severe than for most individuals with lower balances. Similarly, some individuals may place a higher value on their privacy than others. Those individuals will face higher psychological and emotional losses following the invasion of their privacy.

An assessment in the table below should not be read as an assertion that more (or less) severe consequences might not flow from a class of threat.

The table below also recognises that most of the threats outlined already exist under current data sharing practices. However, it should be acknowledged that because the CDR is likely to increase the velocity and immediacy of data transfer, and facilitate the development of richer targets for hackers, it may contribute to increased frequency, likelihood and severity of negative consequences of these threats.

Simple Consumer Data Right model – Risk Assessment

The following table considers the potential privacy threats and likely consequences if data were shared in a manner similar to the simple CDR model scenario outlined above.

The assessments of severity are based on the application of CDR to banking data. The severity of consequences of a threat being realised is highly dependent upon the data sets involved. Banking is a high risk data set. For example, banking transaction data may include insights into an individual's location, health purchases, relationships, or political or other associations; this may particularly be the case when this data is combined with other data sets (such as telecommunications or social media data).

Separate privacy impact assessments will occur as part of the sectoral assessments for each new sector subject to the regime.

Examples provided in the table below are purely for illustrative purposes – to help the reader understand the nature of the threat. They do not provide an indication of the most likely severity of case.

For example, an example might highlight a more severe scenario that could occur (for example, the example of political use of a person's data in stage 2.1) – notwithstanding the likely consequences might be lower (or even higher). As noted above, this table does not take into account risk mitigation strategies in the CDR framework – see tables 8 and 9 below for an assessment of the likelihood of these threats occurring once mitigation strategies are applied.

Table 6: Privacy Impacts Table – Simple CDR Model

Stage	#	Threat	Likelihood	Severity	Risk	Threat under current data sharing?
Stage 1: Individual engages with data recipient	**1.1**	*A third party may pose as the accredited data recipient in order to acquire the individual's information directly from the individual.* • E.g. A non-accredited financial application may pretend to be BetterDeals and request that Naomi send them her email address and phone number. NB: The threat of the third party trying to acquire the individual's data from the data holder is dealt with further below.	Possible	Moderate[36]	Medium	Y
	1.2	*A third party may use a false identity to acquire information from the accredited data recipient that the accredited data recipient had previously collected directly from the individual.* • E.g. Amanda may pretend to be Naomi and engage BetterDeals to get Naomi's email address and phone number.	Possible	Moderate	Medium	Y

[36] For Threats 1.1 and 1.2, the risks associated with the acquisition of authentication information (e.g. banking credentials) are dealt with separately below. This contributes to the potential severity of the threat being categorised as moderate rather than major or extreme.

	1.3	*The individual may engage an accredited data recipient who instead seeks data outside the CDR system.* • E.g. Naomi may engage with a tech company believing that access to her data will be obtained through the regulated framework of the CDR. The data recipient instead obtains her personal information through screen scraping. • E.g. Naomi engages with a financial advisor who obtains her data through existing bilateral arrangements with NN Bank.	Possible	Minor	Low	N
Stage 2: Individual authorises use and collection of data	**2.1**	*The individual may authorise the accredited data recipient to use or collect their data in a way that they did not genuinely intend.* • E.g. Naomi may authorise the use of the data for 'marketing purposes' not appreciating that this will result in her receiving unwanted notifications about restaurants to try based on preferences revealed in her transaction data. • An example of a major (but less likely) negative consequence may be that Naomi may authorise the use of the data for 'research purposes' not appreciating that this purports to authorise analysis of her political views. • Another example is that Naomi may consent to her data being used to assess her for an insurance policy without realising that the insurance provider may use the data to assess her price sensitivity, rather than simply pricing for risk.	Almost Certain	Minor	Medium	Y
	2.2	*The individual may inadvertently authorise a level of access or use of their data beyond what is required for the services they are seeking.* • E.g. Naomi does not bother to read the consent terms of BetterDeals	Almost Certain	Minor	Low	Y

	assuming that they only authorise the collection of data for providing the comparison service she desires. By authorising excessive collection, Naomi may face greater privacy risks later in the process due to holding risks.				
2.3	*The information that the individual discloses in the course of seeking services may be used or disclosed by the accredited data recipient without authorisation.*[37] • E.g. BetterDeals may use information about what types of services Naomi is seeking to influence Naomi's spending behaviour in the future. • E.g. BetterDeals may disclose information about the types of services Naomi is seeking to a marketing company that sends her targeted advertising messages.	Possible	Minor	Low	Y
2.4	*The accredited data recipient may use the individual's data in an unauthorised manner.*[38] • E.g. BetterDeals decides to on-sell Naomi's data to a third party without her consent, who then uses the data to get insights into Naomi's purchasing habits. • An example of a major (but less likely) consequence is that BetterDeals may decide to on-sell Naomi's data to a third party without her consent, and the third party then uses the data to get insights into Naomi's health	Possible	Moderate	Medium	Y

[37] Authorisation data refers to information that can be obtained from the individual's action of providing consent to the data recipient. This may include things such as the individual's choices with respect to product types, or basic customer information such as their name, or their bank. This type of data may be used for direct marketing purposes.

[38] See Misuse of Individual data section

		status.				
	2.5	*The accredited data recipient may limit the individual's free choice by including contract terms that require access to the individual's data in exchange for a service.* • E.g. BetterDeals may include a consent term providing that Naomi can only receive their services on the condition that Naomi allows them to use her information for the purpose of research to improve its products and services. • E.g. An example of a major negative consequence may be that Nick, a financially disadvantaged consumer, might only be able to receive advice from Betterdeals under an option where he agrees to the on-sale of his transaction data to a third party. Although there is an option to pay an upfront fee, he cannot afford this. NB: This risk should only be read in relation to risks to privacy. These circumstances may also give rise to non-privacy consumer or competition risks.	Almost Certain	Minor	Medium	Y
	2.6	*A non-accredited data recipient may request that the consumer access and download their own CDR data directly, and provide it to the data recipient in exchange for a service.* • E.g. Help Me! Deals (HM Deals) may request that Naomi directly access and download her data from NN Bank and provide it to them, in exchange for HM Deals' services. This means that HM Deals will not have to seek accreditation or comply with the CDR obligations.	Likely	Moderate	Medium	Y
Stage 3: Individual	**3.1**	*The accredited data recipient may direct the individual to a fake website posing as the data holder's website.*	Unlikely	Extreme	High	Y

consents to data disclosure		• E.g. BetterDeals may redirect Naomi to a fake bank so she can give her consent to disclose her banking data. The fake bank could then attempt to phish for her banking credentials, passwords or other personal information.				
	3.2	*A third party may pose as the accredited data recipient to gain access to the individual's authorisation information from the individual; or they may tamper with the accredited data recipient's information systems to do so.* • E.g. A third party could pose as BetterDeals, in order to redirect Naomi to a fake bank, thereby obtaining her authorisation information. • E.g. A third party hacks BetterDeals' app, in order to redirect Naomi to a fake bank, thereby obtaining her authorisation information.	Possible	Extreme	High	Y
	3.3	*A third party may intercept an individual's authorisation (including by hacking the data recipient's system) as it is sent to the data holder.* • E.g. A hacker intercepts the communication between Naomi and her bank, obtaining Naomi's preferences for future services.	Rare	Extreme	Medium	Y
	3.4	*The individual may unintentionally authorise the disclosure of the wrong data to the accredited data recipient.* • E.g. Naomi authorises disclosure of her data relating to her debit card, rather than her credit card data.	Possible	Minor	Low	Y
	3.5	*The individual may accidentally authorise a level of access to their data beyond what is necessary or required for the services they are seeking.* • E.g. Naomi may authorise NN bank to give ongoing access to her credit card transaction data to BetterDeals and not merely on a once off basis	Possible	Moderate	Medium	Y

	as is necessary for them to undertake product comparisons.				
3.6	*The individual may unintentionally authorise the disclosure of the right data to the wrong accredited data recipient.* • E.g. Naomi authorises disclosure of her credit card data to OtherDeals rather than BetterDeals.	Unlikely	Moderate	Low	Y
3.7	*The individual's authorisation to disclose data may not be received by the data holder.* • E.g. NN Bank may not receive Naomi's authorisation to disclose her data to BetterDeals, meaning that she will not receive the comparison service offered by BetterDeals. Naomi's data is not disclosed to anyone.	Possible	Minor	Low	Y
3.8	*A third party may pose as the individual and authorise disclosure of data.* • E.g. Amanda could pose as Naomi and provide authority to Naomi's bank to disclose her data.	Unlikely	Extreme	High	Y
3.9	*The data holder may improperly use or disclose the terms of the authorisation.* • E.g. After becoming aware that Naomi is seeking services from BetterDeals, NN Bank might impose itself on the relationship between Naomi and BetterDeals in order to seek to provide a similar service to Naomi itself. NB: The assessment of 'likely' assumes a broader interpretation of the term improper than merely contrary to law.	Likely	Minor	Low	Y
3.10	*The data holder may seek alternative or additional information from the individual during the disclosure authorisation that is not required for the*	Likely	Minor	Low	Y

		primary purpose of data transfer. • E.g. NN Bank may seek to obtain information about the services that Naomi is seeking from BetterDeals as a condition of transferring her bank data.				
	3.11	*The data holder may obstruct or dissuade the individual from transferring their data to the accredited data recipient.* • E.g. NN Bank may raise unnecessary obstacles to Naomi disclosing her data to BetterDeals when she is looking to change banks.	Possible	Moderate	Medium	Y
Stage 4: Data holder discloses data to data recipient	**4.1**	*The data holder may accidentally send the wrong individual's data to the accredited data recipient.* • E.g. Due to the negligence of NN Bank, Amanda's data may be sent to BetterDeals, instead of Naomi's data, without Amanda's awareness or consent.	Unlikely	Moderate	Low	Y
	4.2	*The data holder may accidentally send the individual's data to the wrong accredited data recipient.* • E.g. Due to the negligence of NN Bank, Naomi's data may be sent to WorseDeals, who may misuse that data.	Unlikely	Moderate	Low	Y
	4.3	*The data holder may accidentally send the wrong individual's data to the wrong accredited data recipient.* • E.g. Due to the negligence of NN Bank, Amanda's data may be sent to WorseDeals without her awareness or consent. WorseDeals may misuse that data.	Unlikely	Moderate	Low	Y

4.4a	*The data holder may intentionally fail to send any, or complete data to the accredited data recipient.* • E.g. NN Bank may choose not to send a year's worth of transaction data and thereby make BetterDeals' product comparisons less accurate.	Unlikely	Major	Medium	Y
4.4b	*The data holder may unintentionally fail to send any, or complete data to the accredited data recipient.* • E.g. NN Bank may erroneously fail to send a year's worth of transaction data and thereby make BetterDeals' product comparisons less accurate.	Possible	Minor	Low	Y
4.5a	*The data holder may intentionally send inaccurate data.* • E.g. NN Bank chooses to send inaccurate transaction data to BetterDeals. In an extreme case, this could mean that Naomi is denied a loan, until she requests correction of her data.	Unlikely	Major	Medium	Y
4.5b	*The data holder may unintentionally send inaccurate data.* • E.g. NN Bank sends transaction data to BetterDeals containing transactions processed by NN Bank in error. In an extreme case, this could mean that Naomi is denied a loan, until she requests correction of her data.	Possible	Moderate	Medium	Y
4.6a	*The data holder may intentionally fail to send the data in a timely manner.* • E.g. In an effort to prevent Naomi from obtaining BetterDeals' services, NN Bank chooses to delay sending Naomi's data. Naomi gives up using the service in frustration as a result.	Possible	Minor	Low	Y

4.6b	*The data holder may unintentionally fail to send the data in a timely manner.* • E.g. NN Bank's systems are unreliable so there is a delay sending data to BetterDeals. Naomi gives up using the service in frustration as a result.	Possible	Minor	Low	Y
4.7	*The data holder may send the data to the accredited data recipient in a format that frustrates its efficient and timely use.* • E.g. NN Bank may scan and send a hardcopy of Naomi's bank statement. This format may not be an appropriate input to BetterDeals' product comparison algorithms.	Likely	Minor	Low	Y
4.8a	*The data holder may intentionally send accurate but misleading data.* • E.g. NN Bank sends Naomi's transactions data. NN Bank is aware that the data does not contain information on payments that have not yet been sent through to NN Bank.	Unlikely	Major	Medium	Y
4.8b	*The data holder may unintentionally send accurate but misleading data.* • E.g. NN Bank sends Naomi's transactions data. The data does not contain information on payments that have not yet been sent through to NN Bank.	Possible	Moderate	Medium	Y
4.9	*A third party may intercept or interfere with the data during transfer between the data holder and the accredited data recipient*. • E.g. A hacker may intercept Naomi's personal data as it is transferred to BetterDeals. They may sell or misuse Naomi's data for a financial gain.	Rare	Extreme	Medium	Y
4.10	*A third party may pose as the accredited data recipient to gain access to the individual's raw transaction data from the data holder.*	Unlikely	Extreme	High	Y

		• E.g. A third party could pose as BetterDeals to request and obtain Naomi's raw transaction data from her bank, NN Bank.				
Stage 5: Data received by data recipient	**5.1**	*The accredited data recipient, their employee or contractor may view or use the individual's data without authorisation.* • E.g. Naomi's ex-spouse works as a data analyst in BetterDeals. They access Naomi's data to potentially identify her location. • E.g. An academic works part-time as a data analyst in BetterDeals. They use Naomi's data as an input to an academic paper.	Possible	Moderate	Medium	Y
	5.2	*The accredited data recipient may misuse the information provided by the individual in a way technically consistent with their authorisations.* • E.g. BetterDeals may use information such as emails, telephone numbers, and other personal details in a way that, while technically consistent with an authorisation, is improper or abusive.	Possible	Minor	Medium	Y
	5.3	*The accredited data recipient, their employee or contractor may disclose the individual's data without authorisation.* • E.g. BetterDeals sells Naomi's data to a data aggregator without permission.	Unlikely	Major	Medium	Y
	5.4	*A third party may access the accredited data recipient's systems and acquire or use an individual's data without authorisation.*	Possible[39]	Major	Medium	Y

[39] Note, the likelihood of attack on accredited data recipient's systems depends on factors such as their scale and the type of data they hold.

		• E.g. BetterDeals has insecure data systems, allowing a hacker to obtain Naomi's credit card or personal details, which they could then use to commit identity theft or fraud.				
	5.5	*The individual may experience increased threats to privacy due to improved insights about the individual enabled by analytics and better access to aggregated datasets.* • E.g. BetterDeals collects personal data from multiple sources (which Naomi has separately authorised). The aggregated data sets are collectively capable of providing far greater detail of Naomi's location than any of the separate data sets. This presents greater risks to Naomi if the data was subsequently stolen or misused.	Possible	Moderate	Medium	Y
Stage 6: Deletion or de-identification	**6.1**	*The accredited data recipient may intentionally or unintentionally fail to delete or de-identify data when required.* • E.g. BetterDeals holds on to data that by law should be deleted as it is no longer necessary for the original use Naomi agreed to. This holding may create additional ongoing risks associated with unauthorised use and disclosure.	Possible	Minor[40]	Low	Y
	6.2	*The accredited data recipient may publically release personal information that has not been properly de-identified, carrying a risk of future re-identification*	Possible	Moderate[41]	Medium	Y

[40] This is an assessment of the harm from unauthorised holding per se. Consequences arising from other privacy threats that ongoing holding may exacerbate are dealt with under those threats.

[41] As Above

	and hence privacy threats. • E.g. BetterDeals sends de-identified data to an academic institution for research purposes which then gets published in a journal. A third party re-identifies individuals from the information published in the journal article.				
6.3	*Data is not deleted or de-identified even though the accredited data recipient is no longer an eligible data custodian.* • E.g., BetterDeals is a company. Its business fails and it is deregistered without liquidation. Control over Naomi's data is lost.	Possible	Moderate[42]	Medium	N

[42] As Above

Additional Consumer Data Right scenarios – Risk Assessment

Table 7: Privacy Impacts of additional CDR scenarios

Scenario	Threats	Examples
Joint Accounts	One joint account holder may authorise the disclosure of CDR data that relates to a different joint account holder without their consent (note that for most personal accounts, each joint account holder is already legally entitled to the account related information).	Pat and Dane hold a joint account together. Pat is the primary user of the joint account. Dane decides to disclose the joint account's transaction data to BetterDeals without first obtaining Pat's consent.
	One joint account holder may prevent the other joint account holder from accessing or disclosing CDR data that relates to them, or may otherwise coerce the other joint account holder when asked for their consent to a particular use of the data.	Pat wants to disclose the joint account's transaction data to a family law practitioner, but is unable to do so without obtaining Dane's consent. Dane has a history of violence.
Silent Parties	Data may relate to and be personal information of other parties. Data collection, use, holding or disclosure may therefore affect the privacy rights of	Naomi transacts with Paul. Naomi's transaction data therefore discloses information about Paul's transactions. Naomi wishes to share this data with her

	other parties. One person's rights in their data may conflict with the rights of other person's rights in that data.	accountant without seeking Paul's permission.
Intermediaries	In relation to receiving, holding and using data, the threats that arise from the use of an intermediary mirror the threats that arise when a data recipient receives, holds or uses data.	An intermediary engaged by BetterDeals to filter raw transactions before the data is sent to it may misuse the data for marketing purposes.
	The threats associated with an intermediary disclosing data are the same as those when a data holder discloses data.	An intermediary may not use a secure form of communication when disclosing Naomi's information to BetterDeals.
Outsourcing to a third party	Both the data holder and data recipients can outsource functions to a third party. The risk of doing so mirrors the risks of the same activities when undertaken by the data holder or recipients. However, they may be amplified by the addition of more handlers of data. Communication threats are also increased as data is transferred between more entities.	BetterDeals outsources their analysis of Naomi's data to a third party, BruerTech. An employee at BruerTech has been secretly accessing data and using it for his own purposes.

Pooling of data and activities	The use of intermediaries and outsourcing to third parties increases the risk of 'honeypots' and single points of failure. However, as intermediaries would specialise in dealing with data, they may have higher protections than smaller CDR participants.	Many FinTechs might use an intermediary to filter data so that they only receive the data sets they require for permitted uses. The systems of the intermediary are compromised.
Non-Accredited Entities	The types of threats associated with CDR data being sent to a non-accredited entity are similar to the threats associated with data being sent to accredited data recipients. However, the likelihood and severity of those threats may vary. The severity and likelihood of various privacy threats is greater where data is transferred through APIs to non-accredited recipients, particularly in respect of vulnerable consumers. This is because of the greater volume, velocity, and useability of data when provided in standardised form through APIs The ACCC has proposed that the first version of the	Naomi authorises an accredited financial budgeting app to provide reports (prepared using CDR data) to a financial counsellor. The financial counsellor is not accredited.

	Rules will not require or authorise an accredited data recipient to disclose CDR data to a non-accredited recipient at the direction of the consumer, in light of stakeholder concerns about such transfers. The ACCC will consider whether to include the ability for consumers to direct the sharing of CDR data to certain non-accredited entities (including professional advisors such as accountants and lawyers) in the next version of the Rules.	
Data transferred overseas	The same types of threats arise in relation to data where it is transferred overseas. However, the likelihood and severity of these threats may be greater when data is transferred to a data recipient overseas due to the potential impediments to enforcing any privacy rights and remedies. However, it should be noted that some overseas jurisdictions have stronger privacy protections than Australia.	Naomi authorises that her data is transferred to a bank in the country, Moneyland. Moneyland does not recognise foreign court or tribunal orders and Naomi is unable to enforce a judgment against the bank when they misuse her CDR data.

Vulnerable and Disadvantaged Individuals

The analysis above considers the privacy threats associated with the CDR from the viewpoint of consumers as a single class. However, the likelihood and severity of such threats is likely to be different for those subsets of individuals who are vulnerable or disadvantaged. They may experience an increased chance of harm, as well as more severe harm.

Vulnerable and disadvantaged individuals may be affected by different privacy threats in different ways:

- Literacy: Individuals with poor literacy may have difficulty understanding the consent processes and mechanisms. This may lead to the individual authorising the use, disclosure or access to their data which they did not intend. This may in particular occur where data holders and recipients use technical language.
- Digital literacy: Low digital literacy may lead to confusion for individuals. They may find it more difficult to access the CDR and to understand the protections available and the authorisation processes.
- Financial hardship: Individuals who experience financial hardship may be more vulnerable to exploitation as they may be more willing to engage services that have lower privacy standards due to their perceived lack of choice.[43]
- Culturally and linguistically diverse: Different cultural backgrounds may impact individuals' understanding and attitudes towards privacy, consent and technology. There may be cultural factors for some groups, for example, Aboriginal and Torres Strait Islander peoples, that affect the way they engage and therefore the risk they are exposed to.
- Individuals experiencing domestic violence: Individuals who are subject to domestic violence may, for example, be coerced by their abusive partner into unwillingly

[43] Financial Rights Legal Centre and Financial Counselling Australia (2018), joint submission to Treasury on the Treasury Laws Amendment (Consumer Data Right) Bill 2018, available at: https://static.treasury.gov.au/uploads/sites/1/2018/09/t329531-Financial-Rights-Legal-Centre-and-Financial-Counselling-Australia-joint-submission.pdf.

authorising access, use or disclosure of their data, or may be prevented from accessing assistance with the benefit of their own data.

- Minors and individuals with learning disabilities: Individuals who are under 18, and those who have learning disabilities, may face greater threats. They may not fully comprehend the consequences of authorising access, use or disclosure of their data, and may not fully have control of their data.

Vulnerable and disadvantaged individuals may also have more difficulty exercising their rights to avoid or mitigate threats, such as through the use of external dispute resolution, direct rights of action, and seeking assistance from the OAIC. The exercising of some rights requires some familiarity with legal rights and protections, as well as time and other resources.

Authorisation Threats: Genuine consent

Threats to genuine consent

Within authorisation threats, ensuring genuine consent is one of the major challenges to protecting privacy under the CDR. Consent may be given unintentionally or without the individual being fully aware of what they are consenting to or the consequences of their consent. It should also be noted that the CDR consent model is intended to, but cannot ensure valid consent in every case.

The following are factors that influence whether consent is genuine:

- Coercion
  - Consent is not voluntary where there is duress, coercion or pressure that could overpower the individual's will.
  - Coercive conduct may originate from the data holder or recipient; or from a third party, such as an abusive domestic partner.
  - In the case of joint account holders, individuals may be at risk of unwillingly consenting to transfers that the other account holder advocates for. Likewise, a person who wants to transfer their data to a third party in order to obtain assistance may be coerced into not consenting to disclosure.

- Imbalance of power with service providers (including conditionality in service provision)
  - An inability to access a service without consenting (to the collection, use or disclosure of data) does not make consent involuntary per se. Indeed, in some cases, consumers are happy to 'pay' for a service using their data. However, depending upon the significance of the impacts of not being able to access the service, consent may not be 'free', and in extreme cases, consent may not be voluntary.
  - There may be more significant risks where there is an imbalance of power between a provider of an essential service and a consumer.
- Sufficient information
  - Consent should be supported by sufficient information for the consumer to reasonably understand what they are consenting to, the consequences of consenting and their rights regarding consenting (or not consenting).
- Unbundled information
  - A person may fail to be actually informed if information is not clearly presented in a way that is separated from material extraneous to the consent.
- Non-express or non-explicit
  - Where consent is implied this may negatively impact on whether there is a true and complete understanding of what is being consented to.
- Clarity
  - Consent may be undermined if the consent terms are not readily understandable for a member of the general public (that is, someone without legal or technical expertise).
  - For example, consent terms may not be comprehensible if they are presented in multiple locations, incorporated by reference, or split across separate webpages.
- Ambiguity
  - Consent may be undermined if its meaning is not certain.
- Currency
  - Consent may not be effective if it is not obtained at or prior to the time of (and remains current during) the collection, use, holding or disclosure it relates to.

- Comprehensiveness
  - Consent may be undermined if its terms fail to describe all of the permitted collection, use, holding or disclosure. Examples may aid in true understanding, but may not be sufficient alone.
- Specificity, as to purpose
  - Consent may be undermined if it is not of sufficient particularity to ensure the consumer understands the actual collection, use, holding or disclosures they have authorised. An example of non-specific consent is permission to use data for 'research purposes'.
- Consent minimisation
  - Excessive consents may undermine the effectiveness of consent as a mechanism to exert genuine control over information. This may occur where a party seeks a broader consent (for collection, use, holding or disclosure) than that required for the use anticipated at the time of consent.
- Specificity, as to relying party
  - Consent may be undermined if it is not of sufficient particularity as to the entities who will collect, use, hold or disclose the information. An example is where permission is given for 'any subsequent data recipient to whom the data is transferred.'
- Granularity
  - A failure for consents to be for distinctly different data sets and purposes may undermine the quality of consent as it restricts choice in accepting some matters and rejecting others.
  - A lack of granularity in relation to the request for access that can be made, in addition to undermining consent, may also increase other privacy risks.
  - Where data is provided in pre-determined chunks in excess of what is strictly required for intended uses, this may give rise to transfer, holding and use threats that would not otherwise occur.
-

- Manipulation
  - Where processes for obtaining consent are manipulative, this may impact on the quality of consent.
  - 'Fully informed' consent may still be undermined if the information provided is not balanced and dispassionate. Certain processes (such as use of pre-filled boxes, more onerous steps to reject settings, etc) may also result in lower quality consent.

Consents may be affected by behavioural obstacles to effective assessment and decision making. This may be intentional or unintentional on the part of the person seeking consent. These threats may be mitigated by improved analysis, presentation of options and a positive focus on convenience in processes.

Examples of behavioural obstacles		
Information overload	Status quo bias	Choice overload
Mental accounting	Reference dependency	Relativity bias
Hyperbolic discounting	Salience	Decoy effects

- Diminished capacity to consent
  - The quality or validity of consent may be diminished because of the capacity of individuals.
  - Capacity to consent means that the individual is capable of understanding the nature of a consent decision(including the effect of giving or withholding consent), forming a view based on reasoned judgement and communicating a consent decision. Issues that could affect an individual's capacity to consent include:
    - age;
    - physical or mental disability;
    - temporary incapacity, for example during a psychotic episode or a temporary psychiatric illness.

- Where the individual is a minor, in some circumstances they may also make authorisation decisions that have not been fully informed or genuine.
- The Privacy Act does not specify an age after which individuals can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent. The GDPR provides that people younger than 16 years of age cannot consent without a guardian's involvement, although individual member states may provide for younger age limits provided they are no lower than 13 years of age.

- Capability impediments
  - While a person may have the mental or physical capacity to meaningfully consent, they may nonetheless suffer from other impediments that mean that they are not capable of doing so.
  - They may be impeded in their communications or understanding by language, literacy, education, cultural or other barriers.
  - Consent processes must meet the needs of the broad range of persons who may utilise them. Their development must therefore draw upon a diversity of views and expertise.
  - A key barrier to meaningful consent is the potential for a lack of consumer understanding of their rights and the protections afforded by the CDR system and general privacy laws.
  - The CDR education programs that will be undertaken by the ACCC and the OAIC will help to ensure consumers understand the CDR system. They should be designed with a broad range of consumers in mind. The ongoing design of CDR consent processes will be informed by consumer testing.
- Engagement
  - Even where stakeholders have the ability and knowledge to properly engage in consent processes, there is a significant risk to genuine consent posed by disengagement by consumers with consent processes.
  - Individuals' stated privacy preferences may depart from the preferences they reveal by their conduct in consenting to data collection, use, holding and disclosure.

- Positive friction
  - While negative friction in consent processes can be used to manipulate the outcome of consent processes, a lack of 'positive friction' in decision making regarding consents (when those decisions become too convenient or automated) may also negatively affect the quality of consents.
- Silent parties
  - An individual may be a silent party to a data transfer where their data can be revealed in the information of another individual who has provided consent. For example, where Amanda has transferred money to Naomi, Amanda's details will appear in Naomi's transaction data.
  - Silent parties may be excluded from consent processes. Depending upon the circumstances this may or may not be appropriate.

Specific Threats: Cyber Attacks, Identity theft

The introduction of the CDR may contribute to increased risk when communicating and holding information. In particular, it may result in increased frequency, likelihood and severity of hacking activities.

Although these activities occur frequently with current data sharing models, the CDR may give rise to additional threats due to the following factors:

- An increase in the velocity and immediacy of the data transfer;
- An increase in the number of persons holding (or having access to) information;
- The possible development of richer targets for hackers ('honeypots'); and
  - Honeypots may be particularly prevalent in cases where intermediaries or aggregators collate and store consumer data from a range of data holders.
- Vulnerabilities in communicating with back-end systems existing within APIs that could be more easily exploited.

Hacking activities may have a number of significant consequences, such as direct theft of funds or identity theft.

In particular, identity theft may have significant negative consequences for an individual, for example:

- the consumer may have ongoing problems in dealing with services that require identification;
- unauthorised access to sensitive personal information;
- the consumer may be unable to gain credit because of credit ratings information related to the misuse of their identity; or
- the consumer may have to spend significant time and money changing their identifying information.

Aggregation and enhanced insights

Where multiple data sets are aggregated they may pose greater privacy risks than the mere sum of their individual privacy risks.

Data analysis of aggregated data sets can affect outcomes for the individual – in both negative and positive ways.

For example, banking data sets may, combined with telecommunications data, give rise to far more detailed insights regarding the private behaviours of an individual. The individual may choose to enable the creation of these insights and benefit from them – for example, insights into their spending behaviour may help them to improve their habits. However, these insights may also be subject to misuse – for example, unauthorised insights into political preferences.

Banking data

The first sector to which the Consumer Data Right will be applied is the banking sector.

Banking data is a high risk data set.

The financial information contained in banking data can pose financial risks to an individual – such as the loss of funds through fraud. However, banking data contains far more information than 'mere' financial information.

Banking transaction data contains behavioural information.

It contains information as to where a person has been, what their preferences are, what actions they have taken, their relationships, and what their interactions have been with others.

Many very personal activities involve financial transactions – such as in relation to health care.

Political, religious, and philosophical associations or beliefs may be evidenced by financial records. A person's sexuality or sexual activity may be disclosed. Financial records may reveal insights into a person's professional, trade or trade union associations. They may reveal criminal or other improper activities.

Many financial transactions relate to a person's immediate or extended family, including children. Likewise they may relate to the location or other characteristics of a person's home or the homes of loved ones. Such information may pose great risks in a domestic violence context.

Financial status may be closely linked to people's feelings about their status in the broader community. The misuse or unauthorised disclosure of banking data may therefore cause acute emotional or social harm.

Risk Mitigation

The CDR framework and existing legal protections provide a number of risk mitigation techniques to manage the authorisation, communication and usage threats identified above.[44] These protections in the CDR, including those in the Privacy Safeguards (outlined in the section entitled 'Regulatory framework governing the CDR'), are intended to provide a stronger level of privacy protection than the APPs and the Privacy Act.

Many of the risk mitigants are regulatory in nature. It should be noted that effective enforcement is central to the success of these mitigants.

CDR specific

A1. Privacy Safeguards: The Bill will create a minimum set of Privacy Safeguards for the CDR that may be supplemented by additional protections in the Consumer Data Rules.

CDR data recipients are required to comply with the Privacy Safeguards which are 'hardwired' in the primary legislation and set out the minimum privacy requirements, and data holders are required to comply with some of the Privacy Safeguards in relation to their disclosure of data pursuant to the right. While Privacy Safeguards bear similarities to the APPs, they reflect the more onerous privacy protections required by the CDR framework.

The Privacy Safeguards deal with:

- Privacy policies and compliance arrangements;
- A right for consumers to act on an anonymous or pseudonymous basis;
- Restrictions and transparency in relation to collection of information;
- Dealing with unsolicited information;
- Restrictions and transparency in relation to use and holding of information;
- Restrictions and transparency in relation to disclosure of information;

[44] See Appendix B for diagrams that illustrate the different privacy protections that apply at each stage of the CDR.

- Cross-border disclosures of information;
- Use and disclosure of government identifiers;
- Accuracy and completeness of information, including rights of correction; and
- Security of information.

The ACCC can use its rulemaking powers to further strengthen privacy protections.

A2. Information security standards: Data security and transfer standards will be developed by the Data Standards Chair, setting out minimum requirements that must be met.

The Data Standards Chair will set out data security and transfer Standards containing the minimum information security requirements that CDR participants must meet. Data61 published a full draft of the API standards in December 2018.

These Standards are intended to reduce the risk of unauthorised access to CDR data so that the privacy of individuals will be further protected.

The regime will require the establishment of a Data Standards Advisory Committee which must have at least one consumer representative and at least one privacy representative. This was established on an informal basis in July 2018. Consumer and privacy representation will also occur on the working groups of the Data Standards Body.

Rigorous process and consultation requirements will also be imposed on the Data Standards Body, to facilitate the identification and addressing of privacy threats.

In developing the current draft standards, Data61 has drawn on its own cyber security expertise as well as that of CSIRO's Information Management and Technology team, and the Digital Transformation Agency in relation to trusted digital identity and the Gatekeeper Public Key Infrastructure Framework.

Standards must be developed and assessed against criteria specified in the rules, including their impact on privacy and security of data. The standards will use the mutual transport layer security (TLS) protocol. This includes 'handshake' protocols.

A3. Express consent: Consents to collect, disclose, hold or use data will need to be genuine.

In its December 2018 Rules outline, the ACCC proposed that the Rules will set out requirements to ensure consent is voluntary, express, informed, current, clear, specific as to purpose, unbundled, time limited and easily withdrawn. It is also proposed that the Rules will ensure that consent is given by the relevant person with the appropriate capacity, thereby helping to mitigate authorisation threats.

All consents will be required to be 'active' consents. Consent cannot be given through default settings, pre-selected options, inactivity or silence.

Authorisations for data holders or recipients to collect, use or disclose data will automatically expire after 12 months. Data recipients must remind consumers every 90 days of any ongoing data sharing arrangements that are in place.

Joint account holders will have the power to authorise each other to give their bank authority to disclose banking information. However, the default position will be that both parties will have to consent to any disclosures.

The processes for obtaining consent are currently being developed, incorporating behavioural research commissioned by Data61. The results of that behavioural research have been made available on its website.[45]

Additionally, from 1 July 2019, the ACCC and Data61 will launch a pilot program with the big four banks to test the performance, reliability and security of the Open Banking system. This will include extensive consumer and beta testing of access arrangements, including consent processes, using real consumers.

A4. Data Minimisation Principle

Data recipients will be under a positive obligation to minimise their collection and use of CDR data to the extent that is reasonably necessary to provide the products or services sought by the customer.

---

[45] https://consumerdatastandards.org.au/wp-content/uploads/2019/02/Consumer-Data-Standards-Phase-1_-CX-Report.pdf.

A5. Consents as preconditions to service delivery

An accredited person will be prohibited from requiring consent to collection or use of CDR data as a precondition to them offering any unrelated product or service.

A6. Data is transferred to trusted recipients: The CDR will only require data relating to identifiable individuals to be transferred to accredited data recipients. Accreditation is expected to be tiered according to the threat level of the data in question.

The ACCC will be responsible for the accreditation of data recipients and will set out accreditation requirements in the Rules. In its December 2018 Rules outline, the ACCC proposed that accreditation will be limited to entities who meet minimum requirements (fit and proper person, security, data management, privacy, internal and external dispute resolution process and insurance requirements).

The ACCC has also proposed that to receive accreditation, a data recipient must prove it has adequate practices, procedures and systems in place to manage CDR data and information security threats. The data recipient must provide evidence that it meets the minimum requirements for information security through an independent audit.

The ACCC has proposed that the first version of the Rules will have one general level of accreditation, which will enable an accredited data recipient to receive all CDR data within scope for banking and will therefore be subject to stringent obligations (outlined above). In a subsequent version of the Rules, the ACCC proposes to introduce additional levels of accreditation, including levels of accreditation that accommodate business models that use third party intermediaries to collect and/or hold CDR data. Accreditation tiers aim to ensure that only those data recipients capable of protecting high risk data are able to access it, and to mitigate communication threats.

The ACCC will be empowered to suspend, revoke, downgrade or impose conditions on accreditations. Breaches of domestic or foreign privacy laws (by the entity or its senior management) will be one basis for this power being exercised.

Suspended data recipients will be prevented from collecting further information and will be required to notify all consumers (who may then choose to exercise their rights to withdraw authorisations or require deletion).

Persons who lose accreditation will be required to delete or de-identify CDR data.[46]

Further, generally, small to medium sized enterprises (SMEs) are not currently bound by the Privacy Act. However, this exception will not be available to enterprises that obtain accreditation under the CDR. This means that non-CDR personal information held by these accredited data recipients will be subject to the Privacy Act.

A7. All CDR data transfers between data holders and accredited data recipients are encrypted

The regime will require all communications between data holders and accredited data recipients to be encrypted, greatly minimising communication threats. This will largely address threats to do with interception of data by third parties (see, for example, threat 3.3 in Table 5).

A8. Remedies: It is intended that individuals will have access to external dispute resolution arrangements, leveraging existing sector specific schemes. The OAIC will also be empowered to provide remedies to individuals.

The ACCC will be empowered to recognise existing external dispute resolution schemes in the relevant sector. External dispute resolution provides a low-cost alternative to the court system, and will be accessible by both individuals and small business consumers.

Additionally, individuals and small business consumers will be able to seek individual remedies from the OAIC.

A9. A privacy specific regulator: The OAIC will provide advice and expertise on privacy protection, as well as complaint handling and enforcement for privacy protections. The ACCC will have a complementary strategic enforcement role.

The OAIC will be primarily responsible for enforcing the Privacy Safeguards. It will be able to provide individual remedies to complainants. The OAIC will also advise the ACCC on privacy impacts when the ACCC is conducting sectoral assessments. The ACCC will focus on consumer and competition outcomes and on enforcing the balance of the regime.

[46] This has been proposed by the ACCC in its Rules Outline released on 21 December 2018.

The dual regulator model ensures that all aspects of the CDR will be effectively enforced by regulators with the necessary expertise, and that there is a regulator with a key privacy focus in the system. Note that between the regulators, there will be a 'no wrong door' approach to consumer complaints.

A10. Penalties: Breaches of the Safeguards and Rules carry high penalties that will act as an effective deterrent against misconduct or carelessness.

Breaches of specific Rules and any Privacy Safeguard can attract civil penalties up to, for individuals, $500,000 or, for corporations: $10,000,000; three times the total value of the benefits that have been obtained; or 10% of the annual turnover of the entity committing the breach. These penalties align with the competition law and Australian Consumer Law penalty amounts. These significant penalties are intended to discourage participants from intentionally disregarding the Rules and safeguards.

A11. Broad regulators' powers: The Bill will provide regulators with extensive investigation and enforcement powers.

Regulators will be provided with extensive tools to assist in investigation and enforcement of the CDR, including:

- Criminal penalties
- Civil penalties
- Compensation orders
- Infringement notices
- Injunctive orders
- Director disqualification orders
- Adverse publicity orders
- Enforceable undertakings
- Investigation and auditing powers
- Sectoral assessment/general inquiry powers
- Information sharing

These tools are significant. For example, the ACCC's investigation and auditing powers are crafted to ensure that enforcement actions need not only be exercised in response

to consumer complaints. The ACCC and OAIC have indicated that their regulatory approach will include a proactive audit and compliance program for participants.

The OAIC, ACCC and Data61 have received significant funding to develop, set and enforce privacy protections as part of the Consumer Data Right.

The Government has also provided significant resourcing in the 2018-19 Budget and 2018-19 MYEFO for the ACCC, OAIC and Data Standards Body to ensure a high level of privacy and information security protections. The right will not provide bare 'protections' without the backing of real remedies and enforcement. The Government will provide approximately $90 million and 45 ASL to fund regulators over five years from 2018-19 to 2022-23.

	2018-19	2019-20	2020-21	2021-22	2022-23
Australian Competition and Consumer Commission	6.8	11.2	9.5	9.6	9.2
Commonwealth Scientific and Industrial Research Organisation	4.6	3.8	2.5	2.5	2.5
Office of the Australian Information Commissioner	2.8	3.2	3	3.1	3.1
Total — Expense	**11.1**	**11.2**	**10.4**	**10.5**	**10.5**
Related capital ($m)					
Office of the Australian Information Commissioner	0.9	-	-	-	-
Australian Competition and Consumer Commission	5.4	2.7	1.2	1.2	1.2
Total — Capital	**1.4**	**-**	**-**	**-**	**-**

This funding includes $35.7m, provided for in the 2018-19 MYEFO, for information systems to support the security of the regime, and to bring forward work on the CDR for energy.

A12. Direct rights of action: The Bill provides a right of action for breaches of the CDR. This can form the basis of class actions.

Currently, the Privacy Act does not give rise to a right of action directly to the courts by an aggrieved party.[47] For breaches of the CDR, the Bill will create a direct right of action.

[47] The Privacy Act does not include a direct right of action from damages through the courts, however, allows an individual to seek injunctive relief (s98).

This right will enable individuals to seek court remedies against a CDR participant who breaches the CDR, including the Privacy Safeguards.

Where multiple parties are affected, the direct right of action can form the basis of a class action. This right will exist alongside external dispute resolution mechanisms and the ability for regulators to seek remedies.

Any awards of compensation (including through OAIC and dispute resolution processes) will be backed by requirements for all data recipients to have adequate insurance for breaches of their obligations under the CDR.

A13. Targeted application: The CDR is only applied to a sector after consideration of privacy impacts has taken place.

A sectoral assessment by the ACCC, in conjunction with the OAIC, will be required before data sets and data holders become subject to the CDR. The Treasurer must consider the privacy and confidentiality impacts before a sector is designated. Further, the legislation will empower the Treasurer to make regulations to accompany a designation. This power can be used to ensure that the Rules contain certain requirements, including in relation to privacy. The targeted application of the CDR will assist in ensuring that privacy impacts are at the forefront when a sector is designated.

A14. Rights to withdraw consent or to require deletion and anonymization.

Individuals will be entitled to withdraw their consent to a data holder providing access to a data recipient. The ACCC has proposed that individuals will also be able to withdraw any authority given to a data recipient to collect, use or disclose their data, at any time. It has also proposed that this withdrawal of consent will mean the data recipient is required to ensure that the relevant CDR data is either destroyed or de-identified.

The CDR framework will also require data to be deleted upon all relevant use permissions becoming spent. The requirement to destroy or de-identify data once permissions have lapsed aims to prevent data recipients holding data indefinitely, particularly without the individual's knowledge.

The Rules will specify the circumstances in which deletion or de-identification may occur at either the election of the consumer or of the data recipient. De-identification will not be taken to have occurred unless done in compliance with the OAIC and Data61's *De-identification Decision-making Framework*.

A15. Holding out offence: The Bill will make it an offence for a person to falsely hold out that they have accreditation, or have accreditation at a particular level. There will be significant criminal and civil penalties attached.

The Bill will make it an offence for data recipients to falsely present themselves as accredited or accredited at a particular level. The significant penalties attached will act as a strong deterrent against such conduct.

The ACCC has flagged that it is considering whether to provide that accredited data recipients may include the use of an approved CDR logo (**branding**) to indicate that they are a properly accredited entity. This is intended to reduce the likelihood of data recipients successfully falsely holding out that they have accreditation, by making it easier for consumers to identify when they are engaging with an accredited data recipient.

A16. Misleading or deceptive conduct offence: The Bill will include an offence of misleading or deceptive conduct. There is a corresponding civil penalty provision.

The Bill will create an offence and related civil penalty provision, with significant penalties, to prohibit engaging in misleading or deceptive conduct in relation to the CDR system. This will act as a deterrent for entities that may seek to mislead individuals into compromising their data, and privacy. These provisions primarily target two classes of activities:

1. Impersonating a consumer in an attempt to access data under the system.
2. Misleading a consumer into thinking that they are authorising data transfers under the CDR (or that transfers are occurring pursuant to the CDR data protections) when they are not.

The ACCC has proposed to make rules regulating how data recipients may describe their accreditation status, including that the rules may provide for an approved CDR logo usable only by accredited persons.

A17. Accreditation Register: All accredited entities will be listed on a publicly available register. CDR participants will be required to confirm that entities are listed on the Register before transferring CDR data to them.

The Accreditation Register will be a publicly available resource that both CDR participants and members of the general public will be able to access. The Register will list all accredited entities, and the level to which they are accredited.

CDR participants will be required to confirm, via digital certificates, that entities are accredited and listed on the register before transferring data. Individuals will therefore be assured of the trustworthiness of entities before their data is transferred. They will also thereby confirm that the entity's level of accreditation accords with the type of data that they are seeking.

It is expected that in order to gain accreditation, prospective participants will have to meet specific security standards. Guidance will be provided about how to meet these standards.

Following completion of the procurement process for building the accreditation register, Data61, the ACCC and the selected vendor for the register will work together on the detail of the register, including processes for issuing and managing encryption keys. Strong regard will be paid to the lessons arising from the implementation of the UK's Open Banking initiative.

A18. Strong authentication requirements

The register will, through the use of digital certificates, enable participants within the system to confirm the identity of other participants. Such confirmation will be a mandatory element of any data sharing.

Data holders must also confirm the identity of consumers when obtaining their authorisations to disclose data. The rules provide for strong authentication as defined

by the European revised Payment Services Directive (PSD2) and the European regulatory technical standards for strong customer authentication.

A19. Scope: The CDR framework can potentially apply to a broader range of data than the Privacy Act does, that is, data that relates to either a natural or legal person. SMEs are not exempted from the Privacy Safeguards.

The Privacy Act applies to data that is *about* an identified or reasonably identifiable person.

In contrast, the Privacy Safeguards can apply to specified types of data that *relates* to an identifiable or reasonably identifiable natural or legal person. However, they will only apply to data sets specified as being subject to the CDR.

The ACCC has, for example, determined to exclude dates of birth from Open Banking data sets, due to concerns raised about potential misuse (such as in relation to identity theft).

Any privacy-related Rules can also apply to all CDR data in the system.

The CDR framework will bind all data holders, accredited data recipients and gateways. This means that SMEs will not be exempt from privacy protection obligations. In contrast, the Privacy Act contains an exemption for SMEs.

A20. Use restrictions

The Privacy Safeguards restrict the use of CDR data for direct marketing unless positively permitted by the rules. This restriction on direct marketing will help ensure that subsequent use of data will not occur without the customer's consent, and address usage threats. In its December 2018 Rules outline, the ACCC proposed that the Rules will only permit direct marketing (with consent to direct market) of products or services relating to the product or service for which a consumer has consented to the collection and use of their data.

The ACCC has also proposed that the Rules will not authorise an accredited data recipient to on-sell CDR data.

It is also proposed that the Rules will not permit data recipients to use data to create profiles in relation to parties other than the consumer (e.g. through aggregation of data with common counterparties).

Further, as outlined above there will be a sub-class of intermediary called a designated gateway. Designated gateways will only be able to collect, use and disclose information as specifically provided for in the Rules.

Additionally, the CDR system will not authorise credit reporting agencies to undertake actions that they are otherwise prohibited from doing under the law (e.g. under Part IIIA of the Privacy Act)[48]. This is subject to any regulations made under subsection 56EC(3) of the CDR Bill which allows for the modification of Part IIIA. The primary purpose of this regulation-making power is to resolve any unanticipated conflicts that may arise between the Parts. No regulations are proposed at this time.

A21. Consents dashboards

Both data holders and data recipients will be required to keep records of current and historical authorisations to collect, use and disclose data under the system. They will be required to make available user friendly dashboards to ensure customers have transparency in respect of their use of the CDR.

Initially, information on CDR authorisations will not itself be available through the CDR; however, this may be subsequently provided for to enable use of third party CDR consent management services and access to aggregated views of all CDR authorisations for all data holders and recipients for a given consumer.

A22. A separate CDR privacy policy

Data holders and recipients must have a separate CDR privacy policy which is independent of any existing privacy policy.

[48] This is effected through changes to the laws governing credit reporting rather than through the Consumer Data Right regime itself.

Specific matters that the policy must deal with include: a list of all outsourced data service providers that the firm uses, the nature of their services and the CDR data that is disclosed to them; and a list of overseas recipients to whom data may be disclosed (which must be authorised by the consumer under the restrictions on overseas transfers contained in the Privacy Safeguards), the classes of data that may be disclosed to them and the uses of that data by those recipients.

A23. Breach notification

The CDR Framework extends the Privacy Act breach notification scheme to capture CDR data breaches.

The ACCC can also make additional rules for reporting to regulators. For example, it is proposed that participants will be required to report biannually on all complaints and disputes.

A24. General practices: there will be record keeping, audit trails and notification requirements that are intended to ensure CDR participants comply with best practice.

Participants in the system will be required to maintain records on authorisations (granting, variation and withdrawal), requests and transfers (and failures to transfer) under the system. They will also be required to keep records on outsourcing arrangements. Consumers will have access to these records upon request.

A25. Education: the ACCC and OAIC have received funding for ongoing education of individuals. Data61 has been provided with funding for the education of data holders and recipients.

The ACCC and OAIC will provide education to individuals in regards to the CDR and their rights and protections under the regime. The OAIC will also be empowered to issue guidance on the Privacy Safeguards. Data61 will have responsibility for educating CDR participants in relation to compliance with technical standards for privacy, confidentiality and information security. Data61's education program will include a sandbox to allow data holders and accredited data recipients to develop and test their systems. Education will help to ensure that individuals understand the CDR and are able to use it safely and securely.

A26. Age restrictions: Initially the CDR will only be available to persons older than 18 years of age.

The ACCC's Rules will initially exclude minors from utilising the CDR. This is in contrast to the GDPR, which allows persons older than 16 years of age to exercise the right (with member states able to reduce this age further, although no younger than 13 years of age). The ACCC has indicated that this position will be subject to subsequent reconsideration.

A27. Non-API Access by Consumer Directly/Closed System

In its December 2018 Rules outline paper, the ACCC proposed that data holders will not be required to use APIs when sharing a consumer's data with that consumer directly. Rather, a data holder must enable consumers to make a request to access their CDR data via existing mechanisms on their account(s). This is to create barriers to unscrupulous actors using the consumer to bypass the CDR accreditation requirement.

The ACCC has also proposed that the CDR system will initially be closed to non-accredited data recipients. That is, the first version of the Rules will not require or authorise an accredited data recipient to disclose CDR data to a non-accredited recipient at the direction of the consumer, in light of stakeholder concerns about such transfers. The ACCC will consider whether to include the ability for consumers to direct the sharing of CDR data to certain non-accredited entities (including professional advisors such as accountants and lawyers) in the next version of the Rules.

Behavioural research

This PIA recommends that the ACCC, the OAIC and the Data Standards Body should continue to incorporate behavioural research in the design of the CDR system to ensure that the system works effectively and takes into account *actual* consumer preferences and behaviours regarding the exercise of their privacy rights (recommendation 1). As independent agencies, these bodies have discretion as to what research they undertake and the methods used.

The interim data standards body, Data61, commissioned Tobias and CHOICE to undertake consumer research focusing on consumer understanding of consent processes to inform its guidelines about a standard experience for consumers to consent to the sharing and

monitoring of their data. This research has now been completed and the research report is available on Data61's website.[49] The test group of consumers incorporated different consumer typologies. The study recruited a diverse range of participants to account for diverse needs, scenarios and expectations - with a 50% weighting towards participants considered to be vulnerable or otherwise underrepresented. The recruitment process took account of the following characteristics:

- English, financial and digital literacy;
- cultural and linguistic diversity;
- different life stages;
- income;
- consumers with disabilities;
- gender;
- both consumers and small to medium sized enterprises; and
- a mix of metro, regional and remote consumers.

All participants were required to be financial decision-makers and able to provide consent for themselves. The research was undertaken in three stages, with 10 participants in the first stage, a further 50 in the second stage, and a further 20 in the third stage. Participants were recruited by CHOICE. It is expected that further research will be undertaken throughout the implementation of the CDR.

The Government has also announced that from 1 July 2019, the ACCC and Data61 will launch a pilot program with the big four banks to test the performance, reliability and security of the Open Banking system. Consumers and FinTechs will be invited to participate in these pilots and the ACCC and Data61 will also work closely with other banks who have expressed an interest in participating in Open Banking earlier than originally envisaged. The pilot program will include extensive consumer and beta testing of access arrangements, including consent processes.

[49] https://consumerdatastandards.org.au/wp-content/uploads/2019/02/Consumer-Data-Standards-Phase-1_-CX-Report.pdf.

Existing Mitigants

B1. Privacy Act: The Privacy Act and APPs will continue to operate alongside the CDR.

The Privacy Act and APPs will provide protection where data falls outside the ambit of the CDR. Individuals will be able to access the OAIC's complaints handling process, and the OAIC will retain its investigation capabilities.

B2. Commonwealth Criminal Code: The Code includes offences prohibiting unauthorised access, modification, or impairment of data where there is an intent to commit a serious offence.

Individuals will continue to have access to remedies outside of the CDR framework where their privacy has been breached, or data misused. The Commonwealth Criminal Code currently has offences against unauthorised access to, modification or impairment of data held in a computer, with intent to commit a serious offence against a Commonwealth, State or Territory law. Additionally, there is an offence of dishonestly obtaining or dealing in certain personal financial information. These offences may deter unauthorised access by internal parties (for example, an employee of a data recipient), and provide individuals with remedies.

B3. State criminal laws: All States have criminal laws against accessing restricted data. These offences may deter unauthorised access by internal parties.

Individuals will also continue to have access to State remedies outside of the CDR framework where their privacy has been breached, or data misused. Each State currently has offences of unauthorised access, modification or impairment of data. These offences may deter unauthorised access by internal parties (for example, an employee of a data recipient), and provide individuals with remedies.

B4. Breach of Confidentiality: Banks have additional duties of confidentiality. This is a potential cause of action for individuals to pursue.

Where a bank has inappropriately disclosed an individual's data, they may have breached their duty of confidentiality. Individuals may be able to seek remedy through civil courts via this cause of action.

B5. Tort of Negligence: The common law tort of negligence and the Civil Liabilities Acts across all States provide a cause of action for individuals to seek remedy.

The tort of negligence is an existing cause of action that may be applicable when a CDR participant has negligently dealt with data. Where an individual can show that they are owed a duty of care by the data holder or data recipient, and this duty has been negligently breached, they may be able to seek compensation.

B6. Australian Consumer Law: Part 2.1 Misleading or Deceptive Conduct will allow individuals to bring an action against data recipients where they engage in misleading or deceptive conduct.

The Australian Consumer Law has an existing provision similar to the misleading or deceptive conduct offence that will be created by the Bill. It prohibits businesses from engaging, in trade or commerce, in conduct that misleads or deceives or is likely to mislead or deceive consumers or other businesses, even if the business did not intend to mislead or deceive or no one suffered any loss or damage as a result of the conduct. The prohibition is not limited to the supply of goods or services. Prohibited conduct may include failing to disclose relevant information, and making statements, promises, opinions and predictions. This remedy is available for data both within and outside the CDR framework. State and territory fair trading laws extend this prohibition to individuals.

Concerns associated with the risk mitigants

Some stakeholders have raised concerns that the use of the Privacy Safeguards in some circumstances and the Privacy Act protections in other circumstances will make the CDR system too complex for consumers to navigate and therefore make it difficult for them to enforce their rights.

However, the CDR system is designed to be consumer-friendly. The Privacy Safeguards are principally consent-driven in relation to authorisations for collection, use and disclosure of data. Clear consent requirements will make it easier for consumers to identify where the Safeguards have not been complied with, and therefore to enforce their rights.

A separate privacy regime is justified because of the need for higher privacy protections than those established by the APPs. These protections mitigate threats associated with more

convenient and higher velocity transfers of valuable machine-readable data; and to instil justified high levels of consumer confidence in the use of the system.

To address these concerns about complexity, the Bill was amended following the first round of consultation to ensure that most of the Privacy Safeguards will not apply to data holders, and only the Privacy Safeguards will apply to data recipients in respect of CDR data that they have received.

Concerns were also raised by some stakeholders following the first round of consultation on the Bill that the varied roles of the ACCC, OAIC, and the Data Standards Body created a risk of coordination failure, lacked a single role with responsibility for oversight of the CDR system as a whole, and lacked reporting mechanisms.

While there are different roles assigned to different agencies, the regime does contain a clear hierarchy which facilitates coordination. The ACCC rulemaking ultimately enables it to have oversight and strategic level control of the content and processes for making standards. The complaint handling and enforcement roles of the ACCC and OAIC are clearly differentiated in the Bill, while providing flexibility for each to support the other.

The different roles were proposed and retained because they: allow the CDR system to incorporate important differences in expertise, experience, and values; create a framework of contestability and independence in advice to the Minister; allow for differing styles of industry and consumer engagement; and incorporate differing enforcement roles and styles.[50]

Clear reporting lines are provided through *Public Governance, Performance and Accountability Act 2013* (Cth) frameworks. The frameworks include requirements that entities include their performance of CDR functions in their annual reports. Nevertheless, this creates the risk that the functioning of the CDR system will only be reported on in a fractured manner. When compiling reports, relevant agencies should have regard to ensuring that a holistic picture of the CDR is publicly available, and it may be desirable for

[50] See pages 16 to 31 of the OBR for a more detailed discussion of the differing and complementary strengths and styles of these regulators.

the ACCC to compile the separate reporting into a single report once all agencies have published their annual reports.

The Minister ultimately has oversight of all CDR functions and is responsible to Parliament for the appropriate performance of this role.

The Bill also requires that an independent review of the CDR be conducted by 1 January 2022.

Administrative arrangements allow for additional oversight and co-ordination mechanisms. As is the norm, the Minister will be advised by Treasury in these decisions, and where decisions impact on areas of responsibility of other Ministers, the Minister would be expected to consult with those Ministers and their relevant agencies. The OAIC and ACCC have prepared Memoranda of Understanding regarding their relevant enforcement and educational roles in the CDR, while the Minister will set out their expectations for these processes in an expectations letter.

Practically, it is expected that the close engagement that currently occurs between Treasury, the Attorney-General's Department, the ACCC, the OAIC and the Data Standards Body will continue into the future, with officer level conversations occurring frequently. It is also expected that these agencies will continue to engage with other relevant sector-focused agencies as needed.

Risk Mitigation Strategies

Table 8 lists CDR and other risk mitigation strategies (as set out above) that are applicable to each threat. Risk mitigation strategies have been listed in order of relevance to the specified privacy threat. The table also includes a revised, post-mitigant risk likelihood following from the pre-mitigation risk identified in Table 7. The post-mitigant risk likelihood has been determined using the risk rating matrix detailed above.

Please note that not all mitigants listed apply in every situation that could result in the threat. Further PIAs should consider the mitigants in more detail as they are further developed.

As outlined above, the risk assessments **do not** take into account reputational damage to the CDR system itself, as this is outside the scope of this PIA which focusses on harm to individuals.

Table 8: Risk Mitigation Strategies Table – Simple CDR Model

Stage	#	Potential Privacy Threat	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
Stage 1: Individual engages with data recipient	**1.1**	A third party may pose as the accredited data recipient in order to acquire the individual's information directly from the individual.	Primary: Misleading or deceptive conduct offence, holding out offence, education, strong authentication Other: A2, B1, A8, A9, A11, A12, B6, A10	Possible

Stage	#	Potential Privacy Threat	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
	1.2	A third party may use a false identity to acquire information from the accredited data recipient.	Primary: Strong authentication, misleading or deceptive conduct offence Other: A8, A9, A11, A17, A12, B1, B2, A10, A8, B5, A1	Unlikely
	1.3	The individual may engage an accredited data recipient who instead seeks data outside the CDR system.	Primary: Misleading or deceptive conduct offence, education, Accreditation requirements Other: A8, A9, A10, A11, A12, A15	Unlikely
Stage 2: Individual authorises use and collection of data	**2.1**	The individual may authorise the accredited data recipient to use or collect their data in a way that they did not genuinely intend.	Primary: Consent requirements based on user testing, restrictions on direct marketing, Education Other: A8, A9, A10, A11, A12, A2	Possible
	2.2	The individual may inadvertently authorise a level of access or use of their data beyond what is required for the services they are seeking.	Primary: Consent requirements based on user testing, Restrictions on direct marketing, Education Other: A8, A9, A10, A11, A12, A2	Possible

Stage	#	Potential Privacy Threat	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
	2.3	The information that the individual discloses in the course of seeking services may be used or disclosed by the accredited data recipient without authorisation.	Primary: Privacy Act Other: A8, A9, A10, A11, A12, A16, B6	Unlikely
	2.4	The accredited data recipient may use the individual's data in an unauthorised manner.[51]	Primary: Privacy Safeguards, education (participants), Penalties Other: A8, A9, A11, A12, A3, A14, A16, B6, B5, B6, A15, A20	Possible
	2.5	The accredited data recipient may limit the individual's free choice by including contract terms that require access to the individual's data in exchange for a service.	Primary: genuine consent requirements, education (participants) Other: A8, A9, A10, A11, A12, A15	Possible

[51] See 'Misuse of individual data' section.

Stage	#	Potential Privacy Threat	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
	2.6	A non-accredited data recipient may request that the consumer access and download their own CDR data and provide it to the data recipient in exchange for a service.	Primary: non-API direct access	Possible
Stage 3: Individual consents to data disclosure	**3.1**	The accredited data recipient may direct the individual to a fake website posing as the data holder's website.	Primary: Standards (information security), Misleading or deceptive conduct, Penalties, regulator powers, Remedies, OAIC, Australian Consumer Law Other: A1, A6, B1, A12, B1, B2	Unlikely
	3.2	A third party may pose as the accredited data recipient to gain access to the individual's authorisation information from the individual; or may tamper with the accredited data recipient's information systems to do so.	Primary: Commonwealth Criminal Code, State criminal laws, Holding out offence, Misleading or deceptive conduct, Holding out (branding) Other: A6, A25, A8, A9, A10, A11, A12, A17	Unlikely
	3.3	A third party may intercept an individual's authorisation (including by hacking the data recipient's system) as it is sent	Primary: Standards (information security), Commonwealth Criminal Code, State criminal laws,	Rare

Stage	#	Potential Privacy Threat	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
		to the data holder.	encryption Other: A8, A9, A10, A11, A12	
	3.4	The individual may unintentionally authorise the disclosure of the wrong data to the accredited data recipient.	Primary: genuine consent requirements Other: A14, A25, A2, A21, A20	Unlikely
	3.5	The individual may accidentally authorise a level of access to their data beyond what is necessary or required for the services they are seeking.	Primary: genuine consent requirements, Education Other: A14, A8, A9, A10, A11, A12, A2, A21	Unlikely
	3.6	The individual may unintentionally authorise the disclosure of the right data to the wrong accredited data recipient.	Primary: Standards, Privacy Safeguards Other: A17, A25, A3, A14, A21,	Rare
	3.7	The individual's authorisation to disclose data may not be received by the data holder.	Primary: Standards (information security) Other: A24,, A17, A21	Unlikely

Stage	#	Potential Privacy Threat	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
	3.8	A third party may pose as the individual and authorise disclosure of data.	Primary: strong authentication, misleading or deceptive conduct, Commonwealth Criminal Code, State criminal laws Other:A8, A9, A10, A11, A12, A24, A21	Unlikely
	3.9	The data holder may improperly use or disclose the terms of the authorisation.	Primary: Rules Other: B1, A8, A9, A10, A11,	Unlikely
	3.10	The data holder may seek alternative or additional information from the individual during the disclosure that is not required for the primary purpose of data transfer.	Primary: Rules, genuine consent requirements, Standards Other: A8, A9, A10, A11, A12, A21	Unlikely
	3.11	The data holder may obstruct or dissuade the individual from transferring their data to the accredited data recipient.	Primary: Rules, Standards Other: A8, A9, A10, A11, A12, A16, A3	Unlikely
Stage 4: Data holder discloses	**4.1**	The data holder may accidentally send the wrong individual's data to the accredited data recipient.	Primary: Standards, Privacy Safeguards, Other: A8, A9, A10, A11, A12A24,	Rare

Stage	#	Potential Privacy Threat	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
data to data recipient			B4, B5	
	4.2	The data holder may accidentally send the individual's data to the wrong accredited data recipient.	Primary: Standards, Accreditation Register, Encryption Other: A8, A9, A10, A11, A12, A21	Rare
	4.3	The data holder may accidentally send the wrong individual's data to the wrong accredited data recipient.	Primary: Standards, Accreditation Register, Encryption Other: A8, A9, A10, A11, A21	Rare
	4.4a	The data holder may intentionally fail to send any, or complete data to the accredited data recipient.	Primary: Standards, Privacy Safeguards Other: A8, A9, A10, A11, A12, A241	Unlikely
	4.4b	The data holder may unintentionally fail to send any, or complete data to the accredited data recipient.	Primary: Standards, Privacy Safeguards Other: A8, A9, A10, A11, A12, A241	Unlikely
	4.5a	The data holder may intentionally send inaccurate data.	Primary: Privacy Safeguards, Standards	Unlikely

Stage	#	Potential Privacy Threat	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
			Other: A8, A9, A10, A11, A12, A24	
	4.5b	The data holder may unintentionally send inaccurate data.	Primary: Privacy Safeguards, Standards Other: A8, A9, A10, A11, A12, A24	Unlikely
	4.6a	The data holder may intentionally fail to send the data in a timely manner.	Primary: Privacy Safeguards, Rules, Standards Other: A8, A9, A10, A11, A12, A24	Unlikely
	4.6b	The data holder may unintentionally fail to send the data in a timely manner.	Primary: Privacy Safeguards, Rules, Standards Other: A8, A9, A10, A11, A12, A24	Unlikely
	4.7	The data holder may send the data to the accredited data recipient in a format that frustrates its efficient and timely use.	Primary: Privacy Safeguards, Rules, Standards Other: A8, A9, A10, A11, A12	Rare
	4.8a	The data holder may intentionally send accurate but misleading data.	Primary: Privacy Safeguards, Standards, Other: A8, A9, A10, A11, A12	Unlikely

Stage	#	Potential Privacy Threat	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
	4.8b	The data holder may unintentionally send accurate but misleading data.	Primary: Privacy Safeguards, Standards. Other: A8, A9, A10, A11, A12	Unlikely
	4.9	A third party may intercept or interfere with the data during transfer between the data holder and the accredited data recipient.[52]	Primary: Standards (information security), encryption, Privacy Safeguards, Commonwealth Criminal Code, State criminal laws Other: A8, A9, A10, A11, A12, A15, A17	Rare
	4.10	A third party may pose as the accredited data recipient to gain access to the individual's raw transaction data from the data holder.	Primary: Holding out offence, Commonwealth Criminal Code, State criminal laws, Safeguards, Encryption Other: A8, A9, A10, A11, A12, A16,	Rare

[52] The CDR involves an increase in the velocity and immediacy of data transfer, and the development of richer targets for hackers known as honeypots (particularly aggregators that collate and store significant amounts of customer data). Combined, these factors may contribute to increased frequency, likelihood and severity of hacking activities and cyber-attacks.

Stage	#	Potential Privacy Threat	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
			A2, A17	
Stage 5: Data received by data recipient	**5.1**	The accredited data recipient, their employee or contractor may access or use the individual's data without authorisation.	Primary: Privacy Safeguards, Standards, accreditation. Other: A6, A8, A9, A10, A11, A12, A14, A24, A20	Unlikely
	5.2	The accredited data recipient may misuse the information provided by the individual in a way technically consistent with their authorisation.	Primary: Rights to withdraw authorisations, genuine consent requirements, safeguards, dashboard Other: A6, A8, A9, A10, A11, A12, A25	Unlikely
	5.3	The accredited data recipient, their employee or contractor may disclose the individual's data without authorisation.	Primary: Accreditation, Privacy Safeguards, genuine consent requirements Other: A8, A9, A10, A11, A12, B5, A2	Unlikely

Stage	#	Potential Privacy Threat	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
	5.4	A third party may access the accredited data recipient's systems and acquire or use an individual's data without authorisation.[53]	Primary: Standards (information security), accreditation requirements, Commonwealth Criminal Code, State criminal laws Other: A1, A8, A9, A10, A11, A12	Unlikely
	5.5	The individual may experience increased threats to privacy due to improved insights about the individual enabled by analytics and better access to aggregated datasets.	Primary: Data minimisation, consent as preconditions to service delivery, Privacy Safeguards Other: A14, A25, A8, A9, A10, A11, A12, A3, A6	Unlikely
Stage 6: Deletion or de-identification	**6.1**	The accredited data recipient may intentionally or unintentionally fail to delete data when required.	Primary: Right to withdraw consent or delete, Accreditation, Privacy Safeguards, Withdrawal of authorisation (deletion) Other: A8, A9, A10, A11, A12	Unlikely

[53] This risk may be heightened for data recipients who hold large amounts of data, for example, intermediaries.

Stage	#	Potential Privacy Threat	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
	6.2	The accredited data recipient may publicly release personal information that has not been properly de-identified, carrying a risk of future re-identification and hence privacy threats.	Primary: Privacy Safeguards, Accreditation, standards, genuine consent requirement, withdrawal of authorisation (anonymization). Other: A8, A9, A10, A11, A12, B5	Unlikely
	6.3	Data is not deleted or de-identified even though the accredited data recipient is no longer an eligible data custodian.	Primary: Privacy Safeguards, Rules (relating to cessation of accreditation), Deletion Other: A6, A8, A9, A10, A11, A12	Unlikely

Additional Consumer Data Right scenarios

Table 9: Risk Mitigation Strategies - Additional CDR Scenarios

Scenario	Risk Mitigation Strategies	Risk likelihood following application of mitigation strategies
Joint Accounts	The rules include requirements for both parties to provide consent (although one may allow the other to give consent unilaterally), or for either party to withdraw consent. Privacy Safeguards 5 and 10 also provide requirements for joint account holders to both be notified of the collection and disclosure of CDR data. However, as different threats arise to privacy from joint account holders having too much control over joint data and from not having enough, no mitigation strategy will perfectly mitigate all threats that exist for joint accounts. A trade off exists.	Likely
Silent Parties	Rules may provide requirements for consents by silent parties, balancing the competing data rights of the parties, and may provide rules restricting certain uses of data (e.g. profiling of silent parties).	Possible
Intermediaries	In relation to receiving, holding and using data, the mitigants that apply to threats associated with the use of an intermediary mirror the mitigants that apply to threats	Unlikely

	when a data recipient receives, holds or uses data.	
	The mitigants that apply in relation to an intermediary disclosing data are the same as those for a data holder.	Unlikely
	Designated Gateways will be subject to strong constraints regarding their collection, holding, use and disclosure of data.	Unlikely
Outsourcing to a third party	Both the data holder and data recipients can outsource functions to a third party. The same mitigants apply as those that apply to threats that are created by activities undertaken by the data holder or recipients.	Unlikely
Pooling of data and activities	The use of intermediaries and outsourcing to third parties increases the risk of 'honeypots' and single points of failure. The Privacy Safeguards and Standards are key mitigants in relation to these threats.	Unlikely
Non-Accredited Entities	The CDR rules cannot require data holders or accredited data recipients to transfer CDR data to non-accredited recipients. In the absence of a rule authorising transfer by an accredited data recipient to a non-accredited person, the default under Privacy Safeguard 6 is therefore that transfer to non-accredited recipients is not authorised. However, the ACCC can permit (but not require) transfer to non-accredited recipients, via the Rules. The ACCC has proposed that the first version of the Rules will not authorise an accredited	Minor reduction to threats arising once the data is outside of the CDR system. However, significant mitigants applying to

	data recipient to disclose CDR data to a non-accredited recipient at the direction of the consumer, in light of stakeholder concerns about such transfers. The ACCC will consider whether to include the ability for consumers to direct the sharing of CDR data to certain non-accredited entities (including professional advisors such as accountants and lawyers) in the next version of the Rules. Should the ACCC decide to include this in the second version of the Rules, the range of mitigants that would apply in relation to threats of CDR data being transferred to a non-accredited entity are the same as those that apply to threats associated with the process of transfer to accredited data recipients. As discussed further below, protections would continue to apply in the instances of overseas transfer (under Privacy Safeguard 8), or transfer to non-accredited recipients through outsourcing arrangements. However, no CDR mitigants apply once the CDR data has left the CDR system. In relation to *ongoing handling* of data by non-accredited entities, the CDR system does not apply. Once this data is in the hands of non-accredited recipients, the only mitigants that will apply are the Privacy Act (except where the non-accredited recipient is exempt from the Privacy Act, such as an SME) and other relevant existing mitigants, as discussed under the 'Existing mitigants' section above. While the system does not provide for risk mitigants once the data has been transferred outside of the system, the associated threats are somewhat reduced by the mitigants	prevent inappropriate transfers out of the system.

	that apply at the time of transfer.	
Data transferred overseas	Obstacles to enforcement of risk mitigants may increase the likelihood and severity of threats. The regime provides mechanisms to minimise this increase, such as a broad jurisdictional reach, additional accreditation requirements, potential loss of accreditation, more onerous transfer requirements, maintenance of liability by transferees and insurance requirements. Personal data held in foreign jurisdictions will be subject to foreign regulatory protections, some of which are more rigorous than domestic general privacy laws (e.g. the EU GDPR).	Increased likelihood and severity associated with each type of threat.

Residual risk

The majority of the threats outlined in Table 8 have ratings of 'unlikely' or lower following the application of risk mitigation strategies. It is arguable that this is an acceptable level of residual risk, given the counterbalancing significant benefits associated with the CDR regime. In particular, it should be noted that the CDR provides a safer pipe for data transfer than existing mechanisms. However, these residual risks should be monitored over time, including as part of future PIAs and the scheduled post-implementation review of the CDR.

The ACCC's existing risk mitigation framework will apply to the ACCC's additional statutory functions under the CDR regime, enabling ongoing monitoring of these risks. The ACCC has an Enterprise Risk Management Framework that formalises the ACCC's risk management practices, details policies and strategies to strengthen the ACCC's risk culture and establishes processes to review the ACCC's risk management performance. The ACCC's Corporate Governance Board oversees the ACCC's system of risk management including endorsement of the Enterprise Risk Management Framework. The ACCC's Audit Committee provides independent assurance on risk oversight and management to the Accountable Authority (the Chair of the ACCC) through the Corporate Governance Board.

In relation to the standards, the Data Standards Body chair, supported by the Data Standards Body, has responsibility for reviewing the standards regularly. Additionally, the performance of the Data Standards Chair's functions and powers must be included in the Treasury's annual report. These processes will allow for ongoing consideration of residual risks.

Mitigants That Were Not Adopted

Stakeholders proposed a number of privacy mitigants that were either not adopted in the Consumer Data Right system, or that were partially adopted in a different form. Five key proposals and the reasons they were not adopted are discussed below. Of these proposals, two would require legislative reform if they were to be adopted in the future. The remaining three proposals are possible within the proposed legislative framework and can be adopted through the Rules should evidence suggest that this is the best course of action.

Mitigants that would require further legislative change

General Privacy Act reform and introduction of a Human Rights Act

During the CDR reform process, a number of stakeholders have advocated for overarching reform to the Privacy Act, to introduce protections similar to those provided by the GDPR.

While some stakeholders advocated for this position instead of the CDR reforms, others advocated for it in addition to the CDR reforms. Others proposed that many aspects of GDPR should be substantially replicated within the CDR.

General Privacy Act reform was outside the scope of this project, which was focussed on data portability and provides rights to business customers as well as individuals. The CDR Bill is more targeted than the Privacy Act. It is intended to bring consistency to consumers' experiences of requesting to access and transfer specific data sets, so that they can more easily be made immediately available in a standardised form and therefore at a lower marginal cost.

As discussed above, the fact that CDR data will be more readily available, with data moving through the system with greater velocity and in a more useable format means that the risk profile of data transferred through the CDR is greater than that of much data shared under APP 12 of the Privacy Act currently. This, combined with the need for a high level of consumer confidence regarding the safety of the system, weighed in favour of privacy settings that are stronger than those which should apply generally to personal information throughout the economy.

In considering reforms to the Privacy Act, it is important to remember that the Privacy Act is intended to be of broad application and to cover all instances of collection and use of individuals' personal information (other than by SMEs, and in particular circumstances such as some political purposes). The Privacy Act therefore spans a range of actors, from retail shops, to large multi-national corporations, health providers and the Federal Government; and a range of circumstances, such as online and offline interactions. In contrast, the CDR provides for the narrower range of circumstances relating to the operation of electronic data portability, allowing for better and more targeted solutions. More specialised arrangements (such as allowing only express consent) with greater privacy benefits are not only practicable, but may be implemented without imposing unacceptable levels of regulatory burden or unduly adversely affecting competition, consumer outcomes or innovation.

The proposed CDR privacy arrangements can thus be considered analogous to the existing range of sector- or actor- specific legislation that imposes additional or higher level privacy protections in specific circumstances. For example, state based privacy laws, health records laws, and privacy codes such as the Credit Reporting Code.

Within the CDR system, a number of GDPR-style protections have been or are likely to be adopted. This includes the scope of data being that which *relates* to a person, as opposed to data that is *about* a person; adoption of much of the GDPR definition of consent, including that it be express; rights to be forgotten; binding small-to-medium sized enterprises where they are accredited persons; a direct right of action for individuals; and increased penalties.

It should be noted that elements of the CDR are more restrictive than GDPR. For example, the CDR does not permit non-consent based collection, use and transfer on grounds such as it being within the 'legitimate interests' of the business.

Relatedly, some stakeholders argued for a Human Rights Act to be introduced, with a legal right for an individual or group to sue for breach of their rights, including a breach of privacy or data protection. Broader human rights law reform was outside the scope of the CDR project, for similar reasons to those canvassed above in relation to privacy law reform. However, it should be noted that the CDR system includes a direct right of action for consumers to seek court remedies against a CDR participant who breaches the CDR framework, including the Privacy Safeguards.

Placing elements of protections in the CDR Bill as opposed to the Rules

Some stakeholders have argued that elements of the CDR system such as the definition of consent, bans on on-selling of data, timeliness requirements for notifications of inaccuracies in data or correction of data, and requirements for content of notifications under Privacy Safeguards 5 and 10, should be incorporated in the CDR Bill as opposed to the Rules. This concern is based on the risk that the protections described in the ACCC's Rules Framework paper may be reduced over time.

The protections proposed in the Rules Outline paper are based on the risk levels for financial information, following a long period of consultation with the sector and consumer advocates regarding the appropriate privacy protections in this context. Though it is anticipated that consistent protections will be applied for all CDR sectors, flexibility is required in order to

tailor how the system works in sectors with different existing regulatory systems, data sharing arrangements and business models; to enable the system to evolve as technologies and data sharing approaches evolve; to meet the needs of different consumer types; and to address different threats arising in relation to different data sets. It should also be noted that there is scope for the protections in the Rules to be increased over time.

Rulemaking is subject to ministerial consent and parliamentary disallowance, and mandatory consultation and assessment processes must be followed to ensure that the protections in the Rules remain appropriate.

Mitigants that have not yet been fully adopted, but are possible within the existing legislative framework

It is not currently proposed that the following mitigants be fully adopted. However, they are within the scope of the rule-making power, and as such could be adopted by the ACCC should robust evidence suggest there is a need for them in the future.

Banning other forms of sharing of CDR data

In the CDR legislative consultation process some stakeholders proposed that other forms of data sharing, such as screenscraping, should be banned.

There is a broad range of data sharing arrangements currently in place. The CDR regime cannot meet all of the different tailored requirements that are currently being met by these arrangements. Prohibiting them would have significant negative impacts on consumers and business. However, as the CDR develops it is expected that it will meet the needs currently being met by many of these arrangements. If the CDR is designed and implemented in a way that is efficient, convenient and that inspires confidence in consumers and businesses, it is expected that consumers and business will choose to use the 'safe pipe' that it represents.

Reasons for this proposal also include concerns that individuals may not understand that they are subject to different protections when sharing data through the CDR compared to when doing so under the Privacy Act. Concerns were raised that this could mean that negative outcomes outside of the CDR system undermine individuals' confidence in the CDR.

This is a risk that can be mitigated by using methods other than banning other forms of data sharing. Consumer education and clear branding of CDR transfers should be sufficient to differentiate CDR disclosures from other forms of data sharing. Additional mitigants include

the public register of accredited persons, customers being able to initiate transfers from the data holder end as well as the data recipient end of the transfer, and the CDR Bill including the offences of misleading or deceiving a CDR consumer and holding out as an accredited person.

Other stakeholder concerns related to privacy and security concerns with these other data sharing arrangements, rather than concerns with the CDR per se. Addressing these concerns, if appropriate, is outside the scope of the design of a CDR.

Only authorising certain uses

Some stakeholders have proposed that the CDR should be limited to a range of Government-approved uses. It has been suggested that this should be achieved by creating a taxonomy of approved uses and limiting the use of data to those listed on this taxonomy.[54] Some have suggested that this list should only include uses supported by a majority of respondents to relevant consumer surveys. Proponents of this approach argue that it will ensure that data is used only in accordance with community expectations.

However, a proposal to ban uses only within the specific CDR context runs contrary to the principle of individuals having agency and control over their own data, which is fundamental to the CDR.

In its Rules Outline paper, the ACCC does not create an approved taxonomy of uses, but does propose restrictions on certain uses.

It is proposed that the Rules will authorise an accredited data recipient to use CDR data for the purposes for which the consumer has provided valid consent in accordance with the Rules. However, the Rules will not authorise an accredited data recipient to on-sell CDR data, nor to aggregate data to ascertain the identity of 'silent' parties (parties about which data may be disclosed notwithstanding that they are not the consumer who has consented to the collection and use of their data). It is also proposed that the Rules will prohibit accredited data recipients from using CDR data for the direct marketing of products or services

[54] This should be distinguished from proposals to develop a non-limiting taxonomy of proposed uses for use in approval processes. The purpose of such a taxonomy is to aid in consumer comprehension by creating a short-hand and shared understanding of common uses.

unrelated to the product or service a consumer has consented to the collection and use of their CDR data for.

A closed CDR system

Some stakeholders have argued that the CDR should be a closed system. This has been adopted only to a limited extent. That is, the ACCC has proposed that the first version of the Rules will not require or authorise an accredited data recipient to disclose CDR data to a non-accredited recipient at the direction of the consumer, in light of stakeholder concerns about such transfers. The ACCC will consider whether to include the ability for consumers to direct the sharing of CDR data to certain non-accredited entities (including professional advisors such as accountants and lawyers) in the next version of the Rules.

However, some stakeholders have also argued that the system should be closed in the sense that consumers should be prevented from accessing their own data. They have raised concerns that if consumers have the right to access their own data, with the data provided in a useable form, unscrupulous actors will use the consumer to bypass the accreditation requirement.

It has been suggested that this skirting of the CDR framework could be achieved, for example, by the third party not receiving the data themselves but instead providing the consumer with the software that enables *the consumer* to download the data via an API. CDR data would then be stored on the consumer's device or on cloud storage under an account that is owned by the consumer, but accessed by the non-accredited third party.

Some stakeholders who have raised this concern have proposed that the best method of mitigating this risk is to prevent consumers from accessing their own information under the CDR.

It can be said that, from a privacy rights perspective, it is desirable that consumers have the right to access their information without being required to first provide it to a third party. This is because consumers may wish to access their information simply to know what is being held about them, or may wish to conduct their own analysis of the information without having to disclose this information to others.

It is therefore necessary to consider the balance between the risk of consumers being used as a 'funnel', and the desirability of enabling consumers to access their own information.

While there is a risk that consumers could be used to funnel information, there are methods to mitigate this risk other than preventing the consumer from accessing their own data, such as the approach the ACCC has proposed for the first version of the Rules.

The first version of the rules will provide that data holders are not required to provide consumers access to their data through an API in standardised formats. Data holders will instead be required to enable consumers to make a request to access their CDR data via existing mechanisms on their account.

Greater friction will be introduced where the consumer accesses this information themselves. Additionally, education and clear branding of CDR transfers would ensure consumers know that when they are transferring this way, they are no longer using the CDR (see the 'Risk Mitigation' section for further discussion of branding).

While this would not prevent consumers being used as a funnel in every instance, and as such would not eliminate this risk, it would act as a de facto barrier for the majority of consumers who are considering sharing their data with a non-accredited third party. The residual risk would likely be no greater than existing risks associated with direct access under APP 12.

Other issues

APIs

There is a trade-off between simplicity and generality of an API from the developer's perspective, the simplicity of the user experience it leads to, and the amount of general information that can be passed across the API in action. Software development can be easier and the end user experience made more consistent if APIs are more general purpose in nature, so that the one API can be invoked more often when CDR data is transferred. However, general purpose APIs can, by design, lead to more information being passed than is necessary case by case.

Some stakeholders have favoured a higher level of specificity in API standards (and therefore granularity in payloads), in order to limit the data that the data recipient can access to that necessary to provide its service, in order to protect the consumer's privacy. That is, highly

specific APIs can restrict the data being passed back to a calling process, so that the process does not receive data extraneous to its purposes. When general purpose APIs are used, calling processes can find themselves accumulating personal information beyond what is required, and therefore in breach of the data minimisation principle (the requirement that an accredited data recipient minimise its collection and use of CDR data to the extent that is reasonably necessary to provide the products or services sought by the consumer).

More specifically, some stakeholders have suggested making CDR payloads customisable in order to allow consumers to be specific about which data they would like to be disclosed under the CDR. However, there are concerns that an entirely customisable system would be quite complex, causing confusion for consumers and potentially acting as a barrier to their use of the system.

The approach taken by Data61 in its Christmas 2018 working draft of the API standards aligns generally with the level of granularity adopted by the UK in its Open Banking regime. Data61 proposed that the granularity will be subject to ongoing review and in particular will be a factor considered in the statutory review mandated in the legislation for completion by 1 January 2022. The regime is designed to allow the ACCC to readily require changes to the level of granularity (via the rules) if the interests of consumers require this to occur.

Phishing

Some stakeholders have raised concerns that the incidence of 'phishing' will rise once the CDR regime is in force.

Phishing refers to activities directed at misleading a person into believing they are dealing with a trusted party, in order to obtain confidential information by deception. A common example is where a scammer sends emails that claim to be from reputable businesses with the purpose of inducing consumers to disclose passwords.

In the context of the CDR regime, potential phishing examples include where: a third party purports to be an accredited data recipient and requests that the consumer provide their email address and phone number; an accredited data recipient directs the consumer to a fake website posing as the data holder's website, and the fake website then obtains the consumer's credentials; or a third person poses as the accredited data recipient to gain

access to the individual's authorisation information, or tampers with the accredited data recipient's information systems to do so (threats 1.1, 3.1 and 3.2 in table 5).

The CDR includes strong measures to mitigate against the threat of phishing attempts.

In particular, the regime will make it an offence for entities to falsely present themselves as accredited or accredited at a particular level. There will also be a misleading and deceptive conduct offence, prohibiting entities from misleading consumers into thinking that they are authorising data transfers under the CDR when they are not. These offences will carry significant criminal and civil penalties.

The ACCC has proposed to make rules regulating how data recipients may describe their accreditation status, including that the rules may provide for an approved CDR logo usable only by accredited persons.

Accredited data recipients will also be subject to stringent information security requirements.

Some stakeholders have also argued that the form of authentication flow adopted in the standards will affect the likelihood of successful phishing attacks occurring. Some of these stakeholders are particularly in favour of a 'decoupled' approach, rather than a redirect approach or a known channel redirect approach.

At its core, the resolution of the appropriate authentication model involves assessments of the adequacy of information security arrangements. This is being addressed by the Data Standards Body as part of the CDR standards. Data61 has indicated that its current assessment is that at a high level, a pure redirect model will not be supported. Data61 has indicated that any authentication performed by a data provider should be conducted by referring the customer to manually transition to an appropriate existing channel that the customer is already familiar with.

In coming to this position, Data61 also took into account that, even if risks of using redirections in authentication could be adequately mitigated within the CDR, such an approach may result in consumers becoming comfortable with behaviours that if practiced outside the CDR would increase phishing threats in those other contexts.

The ACCC has been provided with significant funding for the implementation of the CDR which includes enforcement of the regime. The ACCC and the OAIC have also received

significant funding for ongoing education of individuals in regards to the CDR and their rights and protections.

De-identification

The CDR regime will require data to be deleted upon all relevant use permissions becoming spent. The requirement to destroy or de-identify data once permissions have lapsed aims to prevent data recipients holding data indefinitely, particularly without the individual's knowledge.

The ACCC has also proposed that individuals will also be able to withdraw any authority given to a data recipient to collect, use or disclose their data, at any time, and that this withdrawal of consent will mean the data recipient is required to ensure that the relevant CDR data is either destroyed or de-identified.

Stakeholders have expressed concerns about the efficacy of de-identification, arguing that there is always a risk of re-identification. They have pointed to several high-profile data breaches that have occurred in recent years as examples of the harm that can occur when identifiable data lands in the public domain.

There is also a risk that different CDR participants would take inconsistent views about what constitutes sufficient de-identification. Accordingly, the ACCC has taken the additional step of proposing that de-identification will not be taken to have occurred unless done in compliance with the OAIC and Data61's *De-identification Decision-making Framework*.

It is also important that data holders revisit de-identification periodically, as technological changes may mean that the level of de-identification that is considered sufficient as at February 2019 may be insufficient in the future.

Recommendations

The risk mitigation strategies outlined above have been carefully designed to address the threats identified in the 'Impacts to Privacy' section. They combine existing protections with new protections that are being written into the legislation and further protections to be considered for inclusion in the Rules and Standards.

In order for the proposed mitigants to adequately protect participants in the CDR system, they will need to be properly implemented and maintained by the relevant agencies.

It is important to acknowledge that although the risk mitigation strategies should, if implemented correctly, appropriately manage and mitigate threats associated with the CDR, they will not altogether eliminate those threats.

The following recommendations relate to the proper functioning of the CDR system, and ensuring the risk mitigation strategies work as they are intended to.

Consumer engagement

Consumers will need to be engaged with the CDR system in order for it to work effectively and to ensure good customer outcomes.

The quality of consumer engagement will be affected by consumer behavioural obstacles. Factors such as how and when the information is presented can mitigate or exacerbate these obstacles.

Periodic behavioural testing of consumer interfaces with the system is essential to ensure that the requirements of the system meet consumers' needs. In particular, such testing may help to determine how to best present consent terms and authorisation flows in order to promote informed decision making by consumers, including vulnerable individuals.

Incorporating behavioural research into the CDR system will also ensure it takes into account *actual* consumer preferences and behaviours regarding the exercise of their privacy rights, noting that these preferences and behaviours will differ among different individuals.

Recommendation 1

The ACCC, the OAIC and the Data Standards Body should continue to incorporate behavioural research in the design of the CDR system to ensure that the system works effectively and takes into account *actual* consumer preferences and behaviours regarding the exercise of their privacy rights.

Ongoing consumer testing by the Data Standards Body, and the pilot program to test the performance, security and reliability of the CDR system, should have particular regard to vulnerable consumer groups. Test groups should be of sufficient size and diversity to provide justified confidence in the safety of consent processes.

Governance

The ACCC, the OAIC and Data61 (which is currently the CDR Data Standards Body), as government agencies or part thereof, are required to report to the Parliament on their performance annually.[55]

It is important for individuals as well as for the success of the CDR that agencies responsible for its implementation conduct ongoing consideration of how their activities are addressing privacy concerns. Agencies should include this in their annual reports for transparency purposes.

For example, the OAIC should monitor and report in its annual report upon the numbers of complaints it receives that relate to CDR privacy issues. It should report generally on how these complaints have been addressed and consider avenues to limit repeat behaviours. Reporting of breaches could include data on factors such as number of consumers affected and estimated cost of the breach.

[55] Available at: https://www.accc.gov.au/publications/accc-aer-annual-report; https://www.oaic.gov.au/about-us/corporate-information/annual-reports/all/; https://www.csiro.au/en/About/Our-impact/Reporting-our-impact/Annual-reports.

Recommendation 2

The ACCC, the OAIC and the Data Standards Body should ensure that their annual reporting includes reporting on the operation of the CDR, particularly relating to privacy, to provide assurance that rules and practices continue to appropriately handle privacy risks. To facilitate this, the ACCC may consider compiling a consolidated annual CDR report, based on the reporting of relevant agencies' CDR functions.

Consent Framework

As identified in the 'Threats to genuine consent' section, obtaining genuine consent is one of the major challenges involved in protecting each individual's fundamental right to privacy under the CDR. Where an individual lacks awareness or understanding of what they are consenting to, there may be considerable consequences for the welfare of that individual.

The proposed CDR legislation outlines high level principles for how a CDR participant should disclose CDR data. The participant should only disclose CDR data when they are authorised by the rules to do so in accordance with a valid consent from the relevant individual.

Further details relating to the definition of valid consent will be included in the Rules. Risk mitigation strategies rest on the assumption that the Rules will require consumer consent to be voluntarily given, express, informed, specific as to purpose, time limited and easily withdrawn.

It is also important that the Rules deal appropriately with issues relating to consent by vulnerable individuals, including minors and those with disabilities or language difficulties.

Recommendation 3

The ACCC should continue to work with the OAIC to ensure that the Rules create a consent framework that ensures consent is genuine, and protects vulnerable individuals.

Data Security and Transfer Standards

As outlined in the 'Impacts on Privacy' section, the CDR may lead to an increase in communication threats, particularly in relation to hacking and cybercrime activities.

This PIA has identified the data security and transfer Standards that will be developed by the Data Standards Body as a key method of mitigating this threat. These Standards are intended to ensure that CDR participants protect data and the privacy of individuals.

To effectively mitigate communication threats, the Data Standards Body should ensure that the Standards are implemented in accordance with the high level objectives set by the legislation.

Further, in developing the Standards, the Data Standards Body should aim to balance competition, innovation and privacy considerations.

The CDR data standards working groups are already operating in a substantially transparent manner. However, further transparency around the working groups' privacy considerations in relation to API design is required.

Recommendation 4

When designing and implementing the Rules and data security and transfer Standards, the ACCC and the Data Standards Body should seek to avoid placing undue weight on the benefits of competition and innovation at the expense of protecting privacy.

It is noted that there is not always a trade-off between these objectives. Strong privacy protections will drive confidence in the system – which is a necessary prerequisite for realising all other objectives.

Additionally, the data standards working groups should increase transparency around the extent to which privacy-by-design is incorporated into their processes. The working groups should commit to periodic review of the API specifications, and be prepared to specify more granular APIs should inadvertent information disclosure become a concern.

Rule making

The CDR supports a flexible rule and standards setting process that allows protections to be tailored to different threats and circumstances – both within and between industry sectors to which it has been applied. This flexibility within the Rules is necessary for a safer, more efficient and effective system. For example, higher risk data sets can be subject to higher security requirements.

However, a lack of consistency may increase complexities and costs associated with privacy compliance. This may hinder consumers' understanding and impede the exercising of their privacy rights.

Recommendation 5

The ACCC and the Data Standards Body should continue to work with the OAIC to ensure that the privacy related Rules and Standards remain largely consistent across designated sectors, with tailoring to particular privacy threats where necessary.

Controlling Access

The information security standards help guard against unauthorised access to a consumer's data by external parties, however they do not mitigate against employees of the data recipient accessing, using or disclosing CDR data without authorisation.

Recommendation 6

The ACCC should consider making rules requiring accredited data recipients to put in place processes to ensure that CDR data held by the data recipient is not inappropriately accessed by the data recipient's employees.

Coordination

The CDR regulatory framework takes a layered approach, with requirements set out in the legislation, rules and technical standards.

Given this layered approach, the legislation, the Rules, and the Standards need to be closely linked to work in conjunction with one another and ensure a properly functioning regulatory system. To ensure interactions work as intended, the Treasury, ACCC, OAIC and the Data Standards Body should maintain regular communication regarding upcoming issues and changes during the simultaneous development of the legislation, Rules and Standards.

Similarly, the framework establishes a dual regulator model for compliance with the law. The OAIC will be primarily responsible for complaint handling with a focus on privacy protection. The ACCC will be primarily responsible for strategic enforcement actions. Between the regulators, there will be a 'no wrong door' approach to consumer complaints. Agencies will need to share intelligence and work cooperatively to be effective.

Recommendation 7

The Treasury, the ACCC, the OAIC and the Data Standards Body should continue to coordinate their activities, and put in place information sharing arrangements and memoranda of understanding as appropriate.

Consumer Education

A key element of a properly functioning CDR system is for participants to understand their rights and responsibilities within it. In particular, the effectiveness of consent mechanisms is highly dependent on consumer education.

Both the OAIC and the ACCC will conduct education programs to ensure participants understand the CDR system.

Participants, industry groups and consumer advocacy groups should contribute to the development and participate in the delivery of consumer awareness and education activities, as appropriate. Importantly, the education program should make consumers aware of privacy risks, as well as the protections that are available to help mitigate these risks.

Education should also be provided to CDR participants to ensure that they are able to comply with the CDR regime. Education programs should be primarily focussed on the

period shortly before and after its commencement in the banking sector on 1 July 2019, but should be ongoing.

Recommendation 8

The CDR education program should include a focus on raising CDR participant and consumer awareness of privacy threats and rights.

Post-implementation assessment

A post-implementation independent review of the CDR will be completed before 1 January 2022. The evaluation will use benchmarks and indicators to assess the benefits and costs of participation in the CDR. The assessment will provide an opportunity for improvements to the CDR to further promote consumer outcomes, including privacy outcomes.

Metrics that could be included in the assessment include the number of privacy-related complaints received by the OAIC, or the frequency of CDR-related data breaches. Including these metrics will provide the Government, rule makers and standard setters with a further opportunity to address privacy risks and add further protections for CDR participants if required.

Recommendation 9

The post-implementation assessment of Open Banking, and the CDR for future designated sectors, should report specifically on privacy relevant metrics such as privacy related complaints and data breaches.

Arrangements should be put in place at commencement so that the post-implementation assessment can be conducted with the benefit of a robust evidence base.

Further PIAs

The CDR is designed to adapt over time (through changes to rules and standards) and be applied to additional sectors (through new ministerial designations).

Applying the CDR system to new data sets in new sectors may present new or increased privacy risks. The legislation requires that assessments of impacts on privacy, and advice on how to address these impacts, be provided to the Minister when proposing new sectoral designations.

Recommendation 10

All significant changes to the CDR legislation or Rules should be accompanied by further PIAs, conducted in accordance with the OAIC *Guide to undertaking privacy impact assessments* and following engagement with privacy and consumer representatives.

Conclusion

The CDR presents some additional risks to privacy of individuals in exchange for other benefits to privacy, competition, convenience and choice. However, the framework includes safeguards to mitigate those risks.

The Treasury Laws Amendment (Consumer Data Right) Bill 2018, together with supporting rules and standards, will expand upon current privacy and security protections available under the Privacy Act and individuals' existing privacy rights.

The Government consulted broadly in developing the CDR, receiving and incorporating the views of a range of consumer and privacy groups into its design. Stakeholders were heavily engaged at each stage of the CDR development, including consultations run by the Productivity Commission, the Taskforce and the Open Banking Review.

This Privacy Impact Assessment has highlighted a range of privacy risks relating to consent, information security and the unauthorised misuse or transfer of data. Some of these risks could lead to substantial financial, personal and emotional loss.

The proposed privacy and information security protections are likely to adequately mitigate these risks.

These privacy protections include the mandatory accreditation of data recipients; the introduction of transfer, security and data Standards; a role for the OAIC in advising on and

enforcing privacy protections; and a range of avenues for customers to seek meaningful remedies for breaches, such as access to external dispute resolution.

The CDR is a consumer consent driven regime and will still require consumers to exercise due care and judgment in relation to their own data, as the mitigants cannot completely eliminate all risks.

Appendices

Appendix A: Modifications to Privacy Law under Consumer Data Right System

Privacy Act compared to proposed CDR protections

	Privacy Act	CDR
What is protected	Personal information, defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.	CDR data is data that is specified in an instrument designating a sector, or data that is directly or indirectly derived from or associated with CDR data, either wholly or in part. Whether the information is true or not, where CDR data relates to a person who is identifiable or reasonably identifiable and is held, or held on behalf of, an accredited recipient or data holder, the Privacy Safeguards apply. 'Relates' is a broader term than 'about'.
Who is bound	Government agencies and private organisations where the organisation had annual turnover of >$3m in the previous financial year.	Accredited persons are bound to treat data in accordance with CDR requirements. Accredited data recipients are a subset of accredited persons, this definition is used where a safeguard applies to someone who has received CDR data. Once a request for disclosure has been received, data holders are bound by Safeguards 10, 11 and 13. They must also comply with Safeguard 1 to the extend it relates to their role within the system.

		Data holders who receive data are bound by the Safeguards in the same manner as other accredited persons, unless the Rules provide otherwise. Designated Gateways are bound by Safeguards 6, 7 and 12.
Key exemptions	*SMEs* Organisations are not bound where turnover was <$3m in the previous financial year, unless they register with the Information Commissioner as choosing to be treated as bound. *Exemption of political acts and practices* The exemption is primarily intended to ensure political parties can maintain databases containing personal information about individual voters. The Commonwealth *Electoral Roll Act 1918* provides registered political parties with access to electoral roll information. *Saving of certain State and Territory laws* Act is not to affect the operation of a law of a State or of a Territory that makes provision with respect to the collection, holding, use, correction or disclosure of personal information (including such a law relating to credit reporting or the use of information held in connection with credit reporting, subject to any regulations) and is capable of operating concurrently with this Act.	*SMEs* SMEs are **not** exempt from the CDR protections if they are a data holder or accredited person. SMEs who are accredited persons lose their Privacy Act exemption in respect of non-CDR data. *The Commonwealth* In so far as it carries on a business, the Commonwealth is bound as if it were a corporation. The Commonwealth will otherwise not be liable to a pecuniary penalty or to be prosecuted for an offence. *State and Territories* States and Territories will be bound to the extent they submit themselves to the regime. They will not be liable to a pecuniary penalty or to be prosecuted for an offence. *Part IIIA of the Privacy Act (Credit Reporting)* The Privacy Safeguards do not limit Part IIIA of the Privacy Act, subject to any regulations to the contrary. Credit reporting bodies will not be authorised by the CDR to act inconsistently with their obligations under Part IIIA of the Privacy Act. To enable this, the Privacy Act is amended at sections 20E, 21G, and 22E to prevent the consumer data rules from being an authorising law.

Principle 1	**Australian Privacy Principle 1—open and transparent management of personal information** Entities must take steps as are reasonable in the circumstances to implement practices, procedures and systems to ensure compliance with the APPs or relevant privacy codes. Entities must also take steps as are reasonable in the circumstances to implement practices, procedures and systems to deal with inquiries or complaints from individuals about the entity's compliance with the APPs or relevant privacy codes. Entities must have an up-to-date and clearly expressed privacy policy and take such steps as are reasonable in the circumstances to make its privacy policy available free of charge and in such form as is appropriate.	**Privacy safeguard 1—open and transparent management of CDR data** *Privacy Safeguard 1 is equivalent to APP1.* All CDR entities must take steps as are reasonable in the circumstances to implement practices, procedures and systems to comply with the Privacy Safeguards and the Rules. CDR entities must also take steps as are reasonable in the circumstances to implement practices, procedures and systems to deal with inquiries or complaints from CDR individuals about the entity's compliance with the Privacy Safeguards and the Rules. CDR entities must have an up-to-date and clearly expressed policy about the management of CDR data and must make its policy about the management of CDR data available free of charge and otherwise in accordance with the Rules.
Principle 2	(a) **Australian Privacy Principle 2—anonymity and pseudonymity** Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter unless the entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves. Entities may also require individuals to identify themselves if it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.	(b) **Privacy safeguard 2—anonymity and pseudonymity** *Privacy Safeguard 2 is equivalent to APP2, but is more restrictive.* Accredited data recipients must give CDR consumers the option of not identifying themselves, or of using a pseudonym, when dealing with the accredited data recipient unless a circumstance specified in the Rules applies.

Principle 3	**Australian Privacy Principle 3—collection of solicited personal information*** An entity must not collect solicited non-sensitive personal information unless the information is reasonably necessary for one or more of the entity's functions or activities. An entity must not collect solicited sensitive personal information unless: the individual consents to the collection of the information and the information is reasonably necessary for one or more of the entity's functions or activities; or any of the exceptions in sub-clause 3.4 apply. An entity must collect personal information only by lawful and fair means. An entity must collect personal information about an individual only from the individual unless it is unreasonable or impracticable to do so.	(c) **Privacy safeguard 3—collecting solicited CDR data** *Privacy Safeguard 3 is similar to APP3, but is more restrictive.* An accredited person must not seek to collect CDR data from a CDR participant under the consumer data rules unless in response to a valid request from a CDR consumer and the accredited person complies with all other requirements in the consumer data rules for the collection of CDR data. This is a civil penalty provision.
Principle 4	**Australian Privacy Principle 4—dealing with unsolicited personal information** If an entity receives unsolicited personal information it must determine within a reasonable period whether it could have collected the personal information under APP3. If the entity could not have collected the personal information under APP3, it must destroy information if lawful and reasonable to do so, or the entity may retain the information by de-identifying the information.	**Privacy safeguard 4—dealing with unsolicited CDR data** *Privacy Safeguard 4 is more restrictive than APP4.* If an accredited person receives, but did not seek to collect, CDR data from a CDR participant, the person must destroy the CDR data as soon as practicable. The accredited person may retain the CDR Data if it is required to retain the CDR data by or under an Australian law or a court/tribunal order. This is a civil penalty provision.

Principle 5	**Australian Privacy Principle 5—notification of the collection of personal information** At or before the time or, if that is not practicable, as soon as practicable after, an entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances: • (a) to notify the individual as reasonable in the circumstances of matters including the identity and contact details of the entity, that information has been collected, • (b) to otherwise ensure that the individual is aware of any such matters.	**Privacy safeguard 5—notifying of the collection of CDR data** *Privacy Safeguard 5 is equivalent to APP5, but is more restrictive.* At or before the time specified in the rules, a person who collects CDR data in accordance with Privacy Safeguard 3 must take the steps specified in the rules to notify the CDR consumers specified in the rules of the collection. This notification must cover the matters specified in the rules for the purposes of this subparagraph. This is a civil penalty provision.
Principle 6	**Australian Privacy Principle 6—use or disclosure of personal information** If an entity holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the entity must not use or disclose the information for another purpose (the ***secondary purpose***) unless: (a) the individual has consented to the use or disclosure of the information; or (b) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is: (i) if the information is sensitive information—directly related to the primary purpose; or	**Privacy safeguard 6—use or disclosure of CDR data** (d) *Privacy Safeguard 6 is more restrictive than APP6.* • *Use or disclosure by an accredited data recipient* An accredited data recipient of CDR data must not use or disclose it unless the use or disclosure is in accordance with a CDR consumers' valid request. An accredited data recipient of CDR data may also use or disclose that CDR data where the use or disclosure is required or authorised by or under the rules, an Australian law, other than the Australian Privacy Principles, or a court/tribunal order and the person makes a written note of the use or disclosure. This is a civil penalty provision.

	(ii) if the information is not sensitive information—related to the primary purpose; or (c) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or (d) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or (e) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or (f) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for enforcement related activities. Exceptions This principle does not apply to the use or disclosure by an organisation of personal information for the purpose of direct marketing, or government related identifiers.	• *Use or disclosure by a designated gateway* A designated gateway of CDR data must not use or disclose it unless the use or disclosure is required or authorised under the rules or by an Australian law, other than the Australian Privacy Principles, or a court/tribunal order and the person makes a written note of the use or disclosure. This is a civil penalty provision. Note: The rules can only authorise Gateways to collect, store, use, or disclose CDR data that relates to consumers where these rules relate to facilitating the transfer of data between data holders and accredited data recipients, or consumers.
Principle 7	**Australian Privacy Principle 7—direct marketing** *Non-sensitive personal information* If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing unless; (a) the organisation collected the information from the individual; and	**Privacy safeguard 7—use or disclosure of CDR data for direct marketing by accredited data recipients** *Privacy Safeguard 7 is more restrictive than APP7, as it treats all CDR data in a similar manner to the treatment of sensitive information under APP7.* An accredited data recipient of CDR data must not use or disclose it for direct marketing purposes unless the use or disclosure is in accordance

	(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and (d) the individual has not made such a request to the organisation. OR the organisation collected the information from: (a) (i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or (ii) someone other than the individual; and (b) either: (i) the individual has consented to the use or disclosure of the information for that purpose; or (ii) it is impracticable to obtain that consent; and (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and (d) in each direct marketing communication with the individual: (i) the organisation includes a prominent statement that the individual may make such a request; or (ii) the organisation otherwise draws the individual's attention to the	with a CDR consumers' valid request or is authorised under the rules. A designated gateway of CDR data must not use or disclose it for direct marketing purposes unless the use or disclosure is required or authorised under the rules. This is a civil penalty provision.

	fact that the individual may make such a request; and (e) the individual has not made such a request to the organisation. *Sensitive personal information* If an organisation holds sensitive personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing unless the individual has consented to the use or disclosure of the information for that purpose.	
Principle 8	**Australian Privacy Principle 8—cross-border disclosure of personal information** Before disclosing personal information to an overseas recipient: • an entity must take steps as are reasonable in the circumstances to ensure that the recipient does not breach the APPs; or, • the entity must reasonably believe the recipient is subject to a law equivalent to the APPs and there are mechanisms the individual can access to enforce that protection; or • the individual must consent to the disclosure after being informed the entity has not taken steps to ensure the recipient does not breach the APPs; or • the disclosure must be required or authorised by Australian law or court/tribunal; or a permitted general situation must exist.	**Privacy safeguard 8—cross-border disclosure of CDR data** *Privacy Safeguard 8 is similar to APP8, with the addition that the overseas recipient must be a person who holds an accreditation, or as otherwise allowed by the Rules.* An accredited data recipient must not disclose CDR data to recipients who are overseas unless: • the overseas recipient is also an accredited person; or • the accredited data recipient takes reasonable steps to ensure the overseas recipient will not contravene the privacy safeguards (and the accredited data recipient remains liable for any contravention of the privacy safeguards by the overseas recipient); or • the accredited data recipient reasonably believe the overseas recipient is subject to a law equivalent to the Privacy Safeguards and there are mechanisms the consumer can access to enforce that protection; or • the conditions specified in the consumer data rules are met.

		This is a civil penalty provision. Note: This subsection applies in addition to the disclosure restrictions above.
Principle 9	**Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers** Entities cannot adopt a Government identifier unless the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions or to fulfil its obligations to a government agency, or if authorised by Australian law or court or tribunal order. Other exceptions also exist.	**Privacy safeguard 9—adoption or disclosure of government related identifiers** *Privacy Safeguard 9 is more restrictive than APP9* Accredited data recipients cannot adopt a Government identifier as their own identifier of a person, unless the use or disclosure of the identifier is authorised by Australian law or court or tribunal order, other than the CDR. This is a civil penalty provision.
	Privacy Safeguard 10 does not have an APP equivalent.	**Privacy safeguard 10 - notifying of the disclosure of CDR data** Where a data holder has responded to a valid request from a CDR consumer and disclosed CDR data under the rules, the data holder must notify the CDR consumers required by the rules Similarly, where an accredited data recipient has disclosed CDR data, the accredited data recipient must notify the consumer as required by the consumer data rules. The consumer data rules may set out which CDR consumer must receive the notification, where there is more than one consumer, what matters must be included in the notification and the time in which the notification must be given. This is a civil penalty provision.

Principle 10	**Australian Privacy Principle 10—quality of personal information**	**Privacy safeguard 11—quality of CDR data**
	An entity must take steps as are reasonable in the circumstances to ensure personal information that it collects, uses or discloses is accurate, up-to date and complete and, if disclosed, relevant. Accurate, up-to-date, complete and relevant, are interpreted having regard to the purpose of the use or disclosure.	*Privacy Safeguard 11 is equivalent to APP10 and creates a process where CDR participants must correct and disclose a corrected version of CDR data when directed by the individual.* A CDR participant for CDR data must take reasonable steps to ensure that the CDR data is, having regard to the purpose for which it is held, accurate, up-to-date and complete when the CDR participant discloses the CDR data in accordance with Privacy Safeguard 6. This is a civil penalty provision. If a CDR participant for CDR data discloses the CDR data pursuant to the CDR and later, the CDR participant becomes aware that some or all of the CDR data was incorrect because, having regard to the purpose for which it was held, it was inaccurate, out of date, incomplete or irrelevant the CDR participant must advise the CDR consumer for the CDR data accordingly, and do so in writing. This is a civil penalty provision. If a CDR participant for CDR data is advised by a CDR consumer for the CDR data that some or all of the CDR data was incorrect when the CDR participant had earlier disclosed it and the CDR consumer requests the CDR participant to disclose the corrected CDR data to the recipient of that earlier disclosure, the CDR participant must comply with the request. This is a civil penalty provision.

Principle 11	**Australian Privacy Principle 11—security of personal information** Entities must take steps as are reasonable in the circumstances to secure personal information they hold from misuse, interference and loss, unauthorised access, modification or disclosure. If an entity holds personal information about an individual and no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.	**Privacy safeguard 12—security of CDR data** *Privacy Safeguard 12 is equivalent to APP 11.* Persons who collect CDR data in accordance with Privacy Safeguard 3 must take the steps specified in the rules to protect the CDR data from misuse, interference and loss, unauthorised access, modification or disclosure. This is a civil penalty provision. If a person collects CDR data in accordance with Privacy Safeguard 3 and any of the CDR data is no longer needed by the person for the purposes permitted under the rules or the Privacy Safeguards, the person must take the steps specified in the rules to destroy or de-identify the redundant data. This is a civil penalty provision.
Principle 12	**Australian Privacy Principle 12—access to personal information** The entity must give the individual access to the personal information about them on the request of the individual within a reasonable period, in the manner requested by the individual if it is reasonable or practicable to do so. The entity may charge not excessive fees for giving access. Access may be refused on a large number of grounds.	*The CDR as a whole is the equivalent of APP12.* No provision of the *Treasury Laws Amendment (Consumer Data Right) Bill 2018* will have any effect until such a rule is in place. The Rule that will give effect to the rest of the CDR, and be the equivalent of APP12, will be contained in the Rules. This flexibility is required in order to tailor how the system works in sectors with differing existing regulatory systems, data sharing arrangements and business models; to enable the system to evolve as technologies and data sharing approaches evolve; to meet the needs of different consumer types; and to address different risks arising in relation to different data sets.

Principle 13	**Australian Privacy Principle 13—correction of personal information**	**Privacy safeguard 13—correction of CDR data**
	If an entity holds personal information and the entity is satisfied that, having regard to the purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, or the individual requests correction, the entity must take reasonable steps to correct the information. If the entity corrects personal information it has previously disclosed to another entity, and the individual requests that the other entity be notified of the correction, the entity must take reasonable steps to notify the other entity of the correction unless it is impracticable or unlawful to do so. If an entity refuses to correct personal information, the entity must give the individual a written notice that sets out the reasons for the refusal and the mechanisms to complain about the refusal. If an entity refuses to correct personal information, and the individual requests the entity to associate a statement with the information that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, the entity must take such steps as are reasonable in the circumstances to do so. Entities must respond to such requests within a reasonable period after the request is made, and must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).	*Privacy safeguard 13 is equivalent to APP 13.* If a CDR participant for CDR data requests a data holder or accredited data recipient correct the CDR data, that person must take the steps specified in the Rules to: • correct the CDR data; or • include a statement with the CDR data, to ensure that, having regard to the purpose for which the CDR data is held, the CDR data is accurate, up to date, complete, relevant and not misleading; and give notice of any correction or statement, or notice of why a correction or statement is unnecessary or inappropriate. This is a civil penalty provision.

Extraterritorial application	**Extra-territorial operation of Act** The Privacy Act, a registered APP code and the registered CR code extend to an act done, or practice engaged in, outside Australia and the external Territories by an organisation, or small business operator, that has an **Australian link.** Note: The act or practice overseas will not breach an APP or a registered APP code if the act or practice is required by an applicable foreign law An organisation or small business operator has an **Australian link** if the organisation or operator is: an Australian citizen; or a person whose continued presence in Australia is not subject to a limitation as to time imposed by law; or a partnership formed in Australia or an external Territory; or a trust created in Australia or an external Territory; or a body corporate incorporated in Australia or an external Territory; or an unincorporated association that has its central management and control in Australia or an external Territory. An organisation or small business operator also has an **Australian link** if all of the following apply: the organisation or operator is not described above; the organisation or operator carries on business in Australia or an external Territory; the personal information was collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice. This means the Commissioner can take action overseas to investigate complaints.	**Geographical application of this Part** *The CDR framework has a broader geographical application than the Privacy Act.* The CDR provisions apply to some cases where there would not be an Australian link for the purposes of the Privacy Act. For example, where data is collected by a foreign company, outside of Australia, on behalf of an Australian registered company or an Australian citizen, the CDR would apply, but the Privacy Act would not. To the extent that the CDR provisions have effect in relation to CDR data held within Australia and the external territories, the CDR provisions apply in relation to all persons (including foreign persons). To the extent that the CDR provisions have effect in relation to conduct relating to CDR data held outside of greater Australia, the CDR provisions only apply if: the conduct is engaged in by (or on behalf of) an Australian person; or the conduct occurs wholly or partly in Australia or the external territories or on board an Australian aircraft or an Australian ship; or the conduct occurs wholly outside Australia and the external territories, and an Australian person suffers, or is likely to suffer, financial or other disadvantage as a result of the conduct.

Notifiable data breaches	All entities subject to the Privacy Act must notify affected individuals and the Australian Information Commissioner following a breach of APP11.1 that poses a likely risk of serious harm.	*The CDR extends the existing notifiable data breaches scheme to breaches of Privacy Safeguard 11 that pose a likely risk of serious harm.* This extends the existing scheme in relation to the customers who must be notified of a breach (that is, all customers whose data is affected), and in relation to the types of data that will require notification if breached (that is, CDR data).
Complaints process	Individuals do not have standing to sue. Individuals must complain directly to the entity who must respond within 30 days, and then may complain to the OAIC in writing. The OAIC may investigate the complaint, and take reasonable steps to conciliate complaints. However, the Commissioner may decide not to investigate further.	*The CDR provides additional complaints handling mechanisms.* Any person affected (including individuals) will have standing to sue for CDR breaches, including in relation to privacy-like protections. Individuals will be able to complain directly to the OAIC about breaches of the Privacy Safeguards. The OAIC may then direct the individual to the relevant industry ombudsman, or handle the complaint themselves. The ACCC will enforce systemic breaches of the CDR and breaches of the Rules.
Consequences for a breach	Following an investigation, the Commissioner may make determinations finding the complaint substantiated and declaring that; • The entity must not repeat such conduct • The entity must take steps to ensure conduct is not repeated • The entity must perform any reasonable act to redress any loss or damage suffered • The individual is entitled to compensation for loss or damage	*The CDR uses existing powers of regulators (the OAIC and the ACCC), with additional powers related to de-accreditation or movement to a lower accreditation tier expected to be provided for in the Rules, additional penalty provisions and increased penalties.* *Civil penalty provisions* Breaches of specific Rules and Privacy Safeguards can attract civil penalties up to, for individuals, $500,000 or, for corporations, $10,000,000; three times the total value of the benefits that have been obtained; or 10% of the annual turnover of the entity committing the

	suffered • That it would be inappropriate for further action to be taken Determinations are non-binding. The Commissioner or complainant may commence proceedings in the Federal Court to enforce the determination. *Civil penalty provisions* Section 13G of the Privacy Act is a civil penalty provision for cases of serious or repeated interference with privacy by an entity. The Information Commissioner may apply to the Federal Court for an order that an entity pay the Commonwealth a penalty. The maximum penalty payable by a corporation is 10,000 penalty units (~$2.1m). To date the Commissioner has not used the civil penalty power. *Rates of compensation* Loss or damage that can be compensated for includes injury to the feelings of the individual and humiliation suffered by the individual. The Commissioner's determinations of compensation for non-economic loss have ranged from $1000 to approximately S20,000 depending on the circumstances.	breach. These penalties align with the competition law and Australian Consumer Law penalty amounts. Persons who suffer loss or damage by reason of conduct done by another person in contravention of s56BN (1) or (2) (misleading or deceptive conduct towards CDR participants) or s 56CC(1) or (2) (holding out that they hold a CDR accreditation, or an accreditation at a particular level, where that is not the case) may also commit criminal or civil offences. *Rates of compensation* Loss or damage that can be compensated for includes injury to the feelings of the individual and humiliation suffered by the individual.

*Note: Analysis focuses on circumstances relevant to APP entities who are organisations as opposed to agencies as this is the most likely comparable scenario to data holders and accredited recipients under the CDR.

Appendix B: Resourcing

The Government has also provided significant resourcing in the 2018-19 Budget and 2018-19 MYEFO for the ACCC, OAIC and Data Standards Body to ensure a high level of privacy and information security protections. The right will not provide bare 'protections' without the backing of real remedies and enforcement. The Government will provide approximately $90 million and 45 ASL to fund regulators over five years from 2018-19 to 2022-23.

	2018-19	2019-20	2020-21	2021-22	2022-23
Australian Competition and Consumer Commission	6.8	11.2	9.5	9.6	9.2
Commonwealth Scientific and Industrial Research Organisation	4.6	3.8	2.5	2.5	2.5
Office of the Australian Information Commissioner	2.8	3.2	3	3.1	3.1
Total — Expense	**11.1**	**11.2**	**10.4**	**10.5**	**10.5**
Related capital ($m)					
Office of the Australian Information Commissioner	0.9	-	-	-	-
Australian Competition and Consumer Commission	5.4	2.7	1.2	1.2	1.2
Total — Capital	**1.4**	**-**	**-**	**-**	**-**

This funding includes $35.7m, provided for in the 2018-19 MYEFO, for information systems to support the security of the regime, and to bring forward work on the CDR for energy.