12 May 2022

Ms Elizabeth Kelly PSM
Secretariat Statutory Review of the Consumer Data Right
The Treasury
Langton Crescent
Parkers ACT 2600
by email: CDRstatutoryreview@treasury.gov.au

Dear Ms Kelly,

Statutory Review of the Consumer Data Right: Issues paper

Thank you for the opportunity to comment on the Statutory Review of the Consumer Data Right: Issues paper. Financial Rights Legal Centre's (**Financial Rights'**) submission will address the five questions put forward in the Issues Paper.

The implementation of the Consumer Data Right (**CDR**) needs serious reconsideration in order to place the interests of the consumer back into the centre of the regime – that is their interest in both obtaining benefits from their own data but also – and more importantly - their interest in a safe, secure and trustworthy data handling regime. Currently the CDR is less a *consumer* data right and more of a right for *business* to access consumer data, perpetuating an over-reliance on a deeply flawed consent and disclosure model.

In summary, the objects of Part IVD of the Act and their implementation need to be reconsidered with safety, security and *consumer* control front and centre of the CDR because:

- consumers are yet to acquire the ability to obtain and use information about themselves as they see fit;
- the object of only allowing accredited parties to access CDR data has been circumvented by allowing the transfer of CDR data to unaccredited "trusted advisers" with fewer consumer protections;
- "safely" has played a subsidiary role to "efficiently" and "conveniently";
- efficiency and convenience have incorrectly been seen as ends in themselves;
- safety has not been included as an object in relation to accessing information about goods and services; and

- expansion of the CDR to action initiation will exacerbate the positive and negative effects of the CDR, making safety even more important.

The existing assessment, designation, rule-making and standards-setting statutory requirements need to be reconsidered since:

- the Privacy Impact Assessment (**PIA**) process has not been conducted early enough to influence outcomes;
- there has been minimal meaningful engagement with consumers and their representatives;
- the complexity of the regulatory regime remains a significant risk for consumers including, ultimately, a lack of engagement and genuine consent; and
- the CDR relies too heavily on disclosure as the principle means of consumer protection.

To bring the CDR back to a core objective focussed on safety, security and consumer control, the following additional reforms to the CDR regime need to be complemented by a series of reforms to the broader legislative context:

- the objects of the Act should be reconsidered to ensure that safety and security in data handling are primary priorities under the CDR regime, with safety included as an object at Section 56AA(b) at a minimum;
- Privacy Impact Assessment should be embedded and implemented into the policy development process at an early enough stage to influence the outcome of the CDR design;
- consumer testing needs to be significantly expanded to include statistically significant sample numbers and including larger numbers of consumers experiencing a range of vulnerabilities;
- consumer representative organisations need to be appropriately resourced to contribute to the development of the Consumer Data Right;
- reliance on disclosure and consent as the primary means of consumer protection needs to be reduced;
- Access to government databases through the CDR should be approached on a case by case basis, with the benefits and risks carefully assessed in each case
- Data from government databases must only be accessed with the consent of the relevant consumers (where it pertains to them personally, or details of their particular property) and should also be shared with the consumer, with an explanation of what the information means and how it is going to be used
- Privacy Safeguard 3 re: collection of solicited personal information needs a "fair collection" requirement;
- Privacy Safeguard 4: Dealing with unsolicited personal information should be bolstered in line with Australian Privacy Principle 4.1 and 4.3;
- Privacy Safeguards 6 and 7 re: Use and disclosure need to include more definitions and remove the "voluntary consumer data" loophole;

- Privacy Safeguard 11 – Quality of CDR Data needs to be amended to apply to collection or use, and introduce the element of relevance in line with Australian Privacy Principle 10.2;
- Privacy Safeguard 13 re: Correction of personal information needs to be strengthened to require corrections irrespective of how a party becomes aware and enable consumer challenges to refusals;
- establish a set of consumer-centric success metrics including consumer well-being, empowerment and choice, safety and security and building trust;
- conduct a cost-benefit analysis identifying direct benefits to consumers and introduce an audit and enforcement program;
- reverse decisions already taken regarding consent and disclosure matters that are unsafe for consumers;
- ban screen-scraping and other unsafe data access, transfer and handling technologies as has occurred in the UK and Europe;
- introduce an offence for firms to use data obtained via the CDR without accreditation
- expand the consumer protections and safeguards required under the CDR to the entire economy via reforms to the *Privacy Act;*
- introduce an unfair trading practices prohibition to the Australian Consumer Law; and
- introduce a data fiduciary obligation, be it specific to the CDR or economy-wide.

Question One Are the objects of Part IVD of the Act fit-for-purpose and optimally aligned to facilitate economy-wide expansion of the CDR?

Most of the objects of the Act as detailed at Section 56AA have not been met under the Consumer Data Right (**CDR**) regime as currently implemented.

The object of Section 56AA(a)(i) has not been met: Consumers are yet to acquire the ability to obtain and use information about themselves as they see fit

The first object outlined by Section 56AA is:

*a) to enable consumers in certain sectors of the Australian economy to **require information relating to themselves in those sectors to be disclosed** safely, efficiently and conveniently:*

*i. **to themselves** for use as they see fit; (**our emphasis**)*

As acknowledged in the review paper the CDR regime has yet to implement a direct to customer data sharing process.

The ability to obtain your own CDR data was supposed to be a fundamental objective of the CDR legislation and Rules. While this right is included in CDR-Banking Rules 3.4(3), the commencement of the obligation to set up a "direct request service" to allow a consumer to request some or all of their own CDR data was deferred until 1 November, 2021. However, in

September 2021 this deadline was removed and the "direct request" aspect of the regime is now deferred indefinitely "… to allow a future consultation process".[1]

The delay in progressing the "subject access" right in CDR-Banking appears partly due to legitimate fears that "forced" and/or "diverted" subject access could be used to circumvent the CDR consumer safeguards – including but not exclusively the Privacy Safeguards. A question remains as to why organisations would submit to the complex and onerous requirements of a CDR regime to obtain CDR data to offer a service if they can obtain the same information by asking or requiring the consumer to request it under "subject access" and then supply it to the organisation, without some or all of the CDR Rules and Privacy Safeguards applying.

Notwithstanding these concerns, the indefinite deferral of the direct consumer request provisions leaves a gaping hole in the CDR scheme. The entire scheme now facilitates third party access to shared data, with no apparent balancing right for CDR consumers to directly access and control their own CDR data.

It should be noted that under Australian Privacy Principle 12 consumers have a right to access their own data. Under the CDR regime as currently implemented for banking, there is no Privacy Safeguard equivalent to this subject access right. This is presumably because it was meant to be a fundamental objective of the CDR regime.

The guidance on the relationship of the CDR Privacy Safeguards and the Australian Privacy Principles is ambiguous about the application of Australian Privacy Principle 12 to CDR data. We therefore cannot be confident that there is *any* subject access right in respect of such data, at least when it is held by APs and ADRs.[2]

We also note that in its response to the Privacy Impact Assessment Update 4, the Australian Government expressly rejected the need for consideration of "direct to consumer requests" in the energy sector.[3]

Consequent to these decisions, consumers remain dependent at least for now, on the weak, highly qualified *Privacy Act* right of subject access (Australian Privacy Principle 12), which can also involve a fee (at the discretion of the entity).

The subject access right in the CDR scheme is also restricted to Data Holders (**DH**), so that once CDR data reaches an Accredited Data Recipient (**ADR**) or any outsourced provider, or the proposed intermediaries, consumers are entirely dependent on the *Privacy Act* provisions, with all the exemptions, exceptions and bureaucracy they entail.

The failure of the regime to provide direct to consumer access to their own data points to fundamental problems with the object and assumptions of the regime.

---

[1] Ibid, Schedule 5, Items 1 and 2, Amending Rules 6.4(3) and 6.6.

[2] OAIC, *Privacy Safeguard Guidelines* 2021, Table at A.27, and paragraph A.33, https://www.oaic.gov.au/__data/assets/pdf_file/0012/8013/privacy-safeguard-combined-chapters.pdf

[3] Australian Treasury, *Privacy Impact Assessment Agency Response* November 2021, https://treasury.gov.au/sites/default/files/2021-11/p2021-223520-agency-response.pdf

Providing consumers with their own data in an efficient and convenient way does not exist in a vacuum and can have both positive and negative consequences in the sectors in which it is introduced.

The objects of the Act and its implementation have focused on these positives – the potential for use cases to promote efficient and convenient switching, choice and improved competition as referenced at Section 56AA.

But it can also have significant negative consequences for some consumers – particularly those experiencing vulnerability and or financial hardship – in the context of a financial services sector that includes players (such as high cost and avoidant credit models, and other financial services targeting financial hardship[4]) who all have an interest in lowering costs and increasing profits through the exploitation of behavioural biases. There remains the real potential for non-accredited parties to simply ask vulnerable and susceptible consumers to download their own CDR data and manually pass them outside of the CDR system in exchange for access to goods and services – all without the protections afforded by the regime.

The current postponement of direct subject access rights demonstrates the difficulties, security risks, and opportunities for regulatory arbitrage that can occur when introducing a new technological tool into an environment that has the potential to simply exacerbate the harm for many consumers in that sector through speed - at the same time as improving outcomes for some other consumers.

Without prioritising the development of a safe and secure data sharing and handling environment as its primary object, the CDR will remain stuck in this dilemma, and be forced to continue to make decisions that play off the interests of a nascent FinTech sector, financial services businesses and more well off consumers, over the interests of consumers experiencing financial hardship and those vulnerable to exploitation. Implementing the recommendations of this submission would assist in addressing the risks of facilitating direct consumer access and allow the regime to fulfil one of its primary objects.

The object of Section 56AA(a)(ii) has been circumvented by allowing the transfer of CDR data to unaccredited "trusted advisers" with fewer consumer protections

The second object outlined by Section 56AA is:

a) to enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed safely, efficiently and conveniently:

i. …

*ii. to **accredited persons** for use subject to privacy safeguards; (**our emphasis**)*

[4] See Senate Economic References Committee Inquiry into Credit and Financial Services targeted at Australians at risk of financial hardship https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Creditfinancialservices/Report

The current CDR regime has developed an accreditation model that is able to fulfil this object. However this object has been fundamentally undermined by the introduction of the concept of so-called "trusted advisers". This has been a concerning development.

In 2021 the government introduced provisions under the rules for some CDR data to be shared with parties who are not accredited under the CDR regime and are not therefore subject to the CDR Rules or CDR Privacy Safeguards. This is clearly contrary to the clearly stated object at Section 56AA(a)(ii).

The PIA Update 3[5] outlined major concerns which were largely dismissed by Treasury in its response[6] giving assurances that to do so would be in the interests of CDR consumers so that the data is more easily shared and that "Trusted Advisers" can only be members of professions which are regulated.

We note the PIA acknowledged that this would "somewhat mitigate this risk" however it went on to state that "those obligations can offer less protection for CDR Consumers than the strong privacy protections imposed under the CDR regime, or under the *Privacy Act*."[7] These include requirements for members to meet fit and proper person tests, to hold specific hold cyber insurance or data breach insurance or be subject to an EDR scheme among others.

"Safely" has played a subsidiary role to "efficiently" and "conveniently"

We note that the key three elements overriding the objects of the Act are that information be "disclosed safely, efficiently and conveniently."

It is our view that the CDR has been implemented in such a way that the safety concerns of consumers – particularly vulnerable consumers - have regularly been trumped by measures intended to remove "frictions" as sought by the FinTech sector and other interested parties.

This was the case with respect to three critical issues:

- joint accounts and consent rules;
- the introduction of the "trusted adviser"; and
- the use of consumer "insights."

These issues were ones where decisions could have been made that either prioritised the safety of consumers or prioritised efficient and convenient processes for CDR participant firms (and presumably the marginal convenience for at least some potential customers). In each of these areas, the decision was made to prioritise the convenience and efficiency needs of CDR participant firms and their ability to quickly "on-board" customers without losing their interest

[5] Maddocks, Consumer Data Right Regime, Update 3 to the Privacy Impact Assessment, September, 2021 https://treasury.gov.au/sites/default/files/2021-10/p2021-213006-pia-maddocks.pdf

[6] Australian Treasury, Consumer Data Right, Privacy Impact Assessment Agency Response October 2021, https://treasury.gov.au/sites/default/files/2021-10/p2021-213006-pia.pdf

[7] Page Maddocks, Consumer Data Right Regime, Update 3 to the Privacy Impact Assessment, September, 2021

rather than the safety of other consumers – particularly vulnerable consumers including those subject to economic abuse or family and domestic violence.

The privacy concerns raised with respect to of each of these and the risk mitigation strategies recommended in the Privacy Impact Assessment Update 3 were dismissed by Treasury. This was largely done to increase engagement with the CDR regime with low participant numbers to date.

Each of these decisions contradict and upend basic privacy and consent principles, even those consent principles already settled within the CDR framework.

By not embedding the object of safety into the implementation of the CDR regime through a privacy-by-design approach, these decisions have the real potential to lead to consumer harm and undermine consumer confidence in the regime.

A common argument put forward by Treasury and industry is that many of the acts that consumer representatives are seeking to address are "already happening" – such as joint account holders sharing their data without consent, people handing over their passwords to accountants and lawyers or other unsafe practices. Accordingly, it is not the role of the CDR to solve those issues.

We respectfully disagree.

The object of the CDR is to introduce a government-endorsed framework that promotes *safe* and secure data handling practices for consumers and businesses. This necessarily requires addressing and resolving unsafe practices that have led to consumer harm. If the CDR is meant to introduce benefits such as increased control over one's data – those benefits must by definition include solving existing control and access problems that adversely impact on a consumer's control over their data. It cannot simply introduce new, discrete and standalone benefits divorced of any other consequence. This is unrealistic.

CPRC research found that 94% of Australian consumers are uncomfortable with how their personal information is collected and shared online and 88% of Australian consumers do not have a clear understanding of how their personal information is being collected and shared[8] Consumers are looking for safe and more securer data handling practices in which they can have confidence to engage with the digital economy. The CDR should be that safe and secure system. If the CDR is not meant to resolve current data handling problems – then what is the point of spending decades and large amounts of money on a framework that simply replicates and exacerbates existing harms borne of poor data handling practices? All such an approach does is help develop an emerging FinTech market to simply recreate and exacerbate the same problems. This does little to serve the consumer interest.

A more realistic approach is required to ensure that there is recognition of the negative (unsafe) effects the CDR can have on the sector's data handling practices and consumer behaviour. This

[8] New research finds Australian consumers want more control over their personal information and expect fair treatment, 2020, https://cprc.org.au/cprc-2020-data-and-technology-consumer-survey/#:~:text=94%25%20of%20Australian%20consumers%20are,is%20being%20collected%20and%20shared.

arises through the CDR's inherent value – speed, consistency and reliability - which can, in and of itself, lead to perpetuating and exacerbating existing harms and introducing new consumer harms. Further, some of the current dangerous practices have emerged because there has been no safe, reliable alternative. CDR should create that alternative.

For example, Financial Rights has raised a number of issues with respect to the application of CDR to the non-banking sector.[9] The recent consultation paper pays scant regard, if any, to the risks and threats that arise for consumers – in a sector that includes significant numbers of business models that actively target people in financial hardship or at least sell higher cost, riskier products. While there may be benefits for some consumers in terms of increased financial inclusion, and potentially improved responsible lending checks, there are a series of significant risks that will arise when CDR is expanded to this sector. It will also provide the means for lenders to circumvent the Comprehensive Credit Reporting (**CCR**) regulations, through improved analysis and inferring of equivalent data rendering the CCR protections useless. These are potential impacts of the CDR on consumers and already-settled regulatory settings that cannot be ignored and need to be considered and directly mitigated.

The CDR should not be seen to be some agnostic, neutral tool that miraculously only produces positive benefits for all concerned. The CDR does not simply duplicate existing processes - it accelerates them and has substantive negative impacts that arise due to its power and speed.

The downgrading of safety as an object via the CDR's implementation also fails to recognise and acknowledge the signal a government-endorsed consumer data regime gives to consumers and what that means for trust and confidence in the system. If consumers are to have ongoing trust and confidence in the CDR, then it must meet higher standards of consumer protection and safety. If not the government's framework will be to blame for the harms that arise, which will lead to a subsequent lack of confidence in the CDR.

Consequently, we remain of the view that there needs to be a full reconsideration of the decisions made with respect to the current CDR Rules regarding:

- joint accounts;
- subject access rights;
- correction of personal information; and
- trusted advisers

with particular focus on the potential consumer harms that may arise, and unique circumstances in the banking and newly designated sectors.

[9] See Joint consumer submission to the CDR Sectoral Assessment for the Open Finance sector – Non-Bank Lending, https://financialrights.org.au/wp-content/uploads/2022/04/220414_CDR_NonBankLending_FINAL.pdf

Efficiency and convenience should not be seen as ends in themselves

One of the assumptions underpinning the CDR is that efficiency and convenience are solely positive impacts and that any and all "friction" needs to be removed.

This belies a fundamental misunderstanding of both the business, environmental and behavioural contexts in which the regime is being implemented.

Efficiency and convenience *can* be positive to consumer outcomes if they are done so *safely*. Where they are not, they can aggravate consumer harms.

For example, frictionless transactions and processes regularly lead to poor decision-making in the financial services sector. The ease of accessing "fast cash" and payday loans via mobile applications leads to significant consumer harm through spiralling financial hardship. The same can be said for mistaken payments in transferring funds to a scammer, or decisions to invest in complex unregulated financial products such as managed investment schemes or unregulated and scam-prone crypto exchanges.

"Friction" can have a positive impact, slowing down decision-making where consumer understanding is low and where there is an over-reliance on disclosure for consumer protection. Some "friction" is therefore desirable to help arm consumers with an ability to more critically engage with financial products and services that may not necessarily be in their best financial interests and avoid potential harm.[10]

This will only be all the more necessary when the CDR framework is expanded to incorporate action initiation. This will introduce more speed to the process, reducing the time for a consumer to make a considered decision, and exacerbate the potential for harms to arise, where the few risk mitigants place the onus on the consumer through disclosure and consent.

Efficiency and convenience are not the be all and end all of the consumer's needs. Safety must be prioritised.

"Safely" should be included as an object of accessing information about goods and services

We note that safety is not included as an objects at Section 56AA(b):

a) to enable any person to efficiently and conveniently access information in those sectors that:

i. is about goods (such as products) or services; and

ii. does not relate to any identifiable, or reasonably identifiable, consumers; and

Accessing information about goods and services should be efficient and convenient but it also needs to be safe. As described above, making choices that can lead to significant financial decisions accelerated through the CDR can lead to increased levels of consumer harm. Efficiency and convenience must be balanced with safety in this context.

[10] See further examples of positive and negative friction in Duncan Jefferies, How 'positive friction' can create better experiences https://www.raconteur.net/customer-experience/positive-friction/

Expansion of the CDR to action initiation exacerbates the effects of the CDR, making safety even more important

Expanding CDR functionality to include action initiation introduces more risks into the data handling system. Some of the risks of write access identified in previous analysis include:

- poor consumer outcomes resulting from speedier payment and account initiation processes including more mistaken payments, lower levels of engagement with one's finances, and subsequent higher levels of debt;
- industry profiling for profit with increased economic inequality and financial exclusion as more granular data allows for finer tuned risk segmentation, and less transparent AI-informed decision-making;
- greater potential for the misuse of data including increased fraud risks, errors, incorrect advice or recommendations arising from conflicts of interest through exclusive deals, commissions or other misaligned incentives that place the interest of the accredited third party over the best interests of the consumer;
- significant ethical issues that arise in respect of any increased functionality. For example there is currently no mechanism to ensure consumers understand exactly how their data will be used in machine or AI-informed learning and decision-making, or how decisions are made or how value will be extracted from it;
- liability and responsibility for mistaken and unauthorised payments made.

These risks must be mitigated from the start otherwise the CDR will again accelerate existing harms and introduce potentially new consumer harms.

Recommendations

1. The objects of the Act should be reconsidered to ensure that safety and security in data handling be primary priorities under the CDR regime. This should at a minimum involve safety being included as an object at Section 56AA(b)

Question Two: Do the existing assessment, designation, rule-making and standards-setting statutory requirements support future implementation of the CDR, including to government-held datasets?

We wish to raise the following concerns with respect to the assessment, designation, rule-making and standards-setting processes to date. These are:

- Privacy Impact Assessment (**PIA**) processes have not been conducted early enough to influence outcomes;
- there has been minimal meaningful engagement with consumers and their representatives;

- the complexity of the regulatory regime, remains a significant risk for consumers including, ultimately, a lack of engagement and genuine consent;
- the CDR implementation over-relies on disclosure and consent as the principle means of consumer protection.

Privacy Impact Assessment process has not been conducted early enough to influence outcomes.

The Treasury-led PIA processes have been conducted, released and responded to at times too late to have any influence on the CDR regime's design.

For example, in July 2021 when the Treasury were consulting on the CDR rules amendment (version 3) regarding the "opt-out" joint account data sharing model, there had yet to be a public and independent privacy impact assessment for the proposals being put forward.

At the time we noted that Treasury's May 2021 proposals for an opt-out consent model for joint accounts were substantially different to the proposals consulted on by the ACCC in late 2020. The ACCC had produced and consulted on an independent privacy impact assessment at the same time as they released their original consultation paper. No such PIA was released by Treasury on the opt-out approach or the new draft rules at the time of consultation.

It was only after this that a "privacy roundtable" was held by Treasury as part of a still to be drafted PIA. However at this stage the PIA's ability to influence the outcome of the process was minimal, a result demonstrated by Treasury's ultimate response to the PIA.

This process is counter to the process expected by the OAIC and counter to good public policy development. The OAIC's Guide to undertaking privacy impact assessments process[11] states:

> *To be effective, a PIA should be an integral part of the project planning process, not an afterthought. It should be undertaken* ***early enough in the development of a project that it is still possible to influence the project design*** *or, if there are significant negative privacy impacts, reconsider proceeding with the project. A PIA works most effectively when it evolves with and helps to shape the project's development, ensuring that privacy is considered throughout the planning process.*
>
> *Making a PIA an integral part of a project from the beginning means that you can identify any privacy risks early in the project and consider alternative, less privacy-intrusive practices during development, instead of retrospectively. Also, consistent and early use of a PIA ensures that all relevant staff consider privacy issues from the early stages of a project.*

Stakeholders had in previous rules updates also been given the opportunity to provide input into a PIA directly to the independent assessor without the presence of Treasury. This did not occur when we met with the independent assessor in 2021 in the course of a process which was attended and run by Treasury.

[11] https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments

That policy development process was reminiscent of the inadequate PIA process Treasury first conducted in 2018 – the last time Treasury had carriage of the CDR.[12] In that first PIA, Treasury decided not to outsource the development of the PIA to external independent consultants and conducted the PIA themselves. This too was not in keeping with the recommendations of the OAIC in its PIA guidelines. Treasury at the time relented to criticism of this flawed process and engaged an independent PIA to take place.[13]

It is therefore unfortunate that Treasury chose not to undertake an independent PIA for the joint accounts issue at a time early enough "to influence the project design." This should have occurred at the same time as the May 2021 consultation on the opt-out approach proposal and released with responses at the time any new draft rules were released – as occurred with Version 2 of the CDR Rules under the ACCC.

Given the critical importance of the joint account issue and the decision to move forward with an opt-out consent model in direct contradiction of the consent principles, it was incumbent upon Treasury to pause and delay any introduction of new rules, conduct an appropriately independent PIA with input from all stakeholders including consumer representatives, and develop a joint account policy that fully addresses the privacy risks of sharing joint accounts.

By relegating the importance of the PIA process to an afterthought, the object of the regarding safety was sidelined for efficiency and convenience.

Minimal meaningful engagement with consumers and their representatives

For a reform ostensibly aimed at consumers, there has been minimal meaningful engagement with consumers and their representatives.

While there has been some limited Customer Experience (**CX**) testing conducted with a small number of consumers[14] this needs to be significantly expanded to include statistically significant sample numbers and including working with consumers experiencing a range of vulnerabilities – including but not limited to:

- older Australians
- people with a disability
- people with experience of family violence and/or economic ;
- culturally and linguistically diverse communities

[12] See Draft Treasury Privacy Impact Assessment Consumer Data Right December 2018 https://cdn.treasury.gov.au/uploads/sites/1/2018/12/CDR-PIA.pdf

[13] See Consumer Data Right: Maddocks, Privacy Impact Assessment (December 2019) https://treasury.gov.au/publication/p2019-41016

[14] Consumer Data Standards, Consumer Experience Research Phase 3: Round 3 – Joint Accounts and Deidentification and Deletion, April 2020, p. 36. https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2020/05/CX-Report-_-Phase-3-_-Round-3.pdf https://consumerdatastandards.gov.au/engagement/reports/reports-cx/

- people with literacy levels;
- Aboriginal or Torres Strait Islanders; and
- people experiencing financial distress or hardship.

Nor was there any significant engagement with Australian consumers in the development of the rules, standards and other CDR settings.

There has been minimal resources provided to support consumer representative organisations (including our own) to contribute to the development of the CDR policy settings. Attending and contributing to the large number of meetings, workshops, consultations on rules development, standard setting, CX and UX development is simply not possible for resource -limited consumer organisations and our engagement has to date been subsequently limited and selective

Consumer organisations like our own already work under severely constrained and shrinking resource environments that need to prioritise front line service provision as per funding agreements. Where any policy development work is possible in a consumer organisation, solving areas of current harm – not potential future harm that a reform like CDR represents - is necessarily prioritised due to limited resources.

Without substantial increased consumer representative input and consumer testing, the CDR's design is likely to continue to over-rely on the FinTech sector and financial services firms to speak for what *they* believe the consumer wants rather than actual consumers and their independent representatives. The FinTech and financial services sector view of the consumer perspective is far from self-interested and is inevitably seen through a profit motive lens, rather than developing the CDR to address *genuine* consumer needs.

We recommend that if the consumer data right is to be developed with the consumer at the centre of its design, consumer representative organisations need to be properly resourced to provide the consumer voice to the process.

The complexity of the regulatory regime, remains a significant risk for consumers including, ultimately, a lack of engagement and genuine consent

The CDR regime has been characterised as an "ecosystem", with an ever-increasing number and diversity of CDR players[15]. Initially included were consumers, accredited persons (**APs**), accredited data recipients (**ADRs**), data holders (**DHs**) and designated gateways (**DGs**)[16]. In addition, and as the regime has evolved, there is a range of further roles, including "secondary user", "CDR representative", "trusted adviser", " insight recipient", "enclave provider", "affiliate", "sponsor" and "associate". We note too that the CDR rules for the energy sector, issued in

[15] The term "CDR participant" cannot be used as it has a defined meaning – including only Data Holders and Accredited Data Recipients. Similarly, CDR entity has a defined meaning – including DHs, ASRs and DGs.

[16] As at 25 January 2022, 72 organisations are accredited as CDR Data Holders (with 30 additional "brands"), but only 26 as ADRs. The Office of the Australian Information Commissioner, CDR Privacy Safeguard Guidelines, Version 3.0 (June, 2021), state "there are currently no designated gateways", A.37 Note.

November 2021, introduce a further concept of peer-to-peer (**P2P**) data sharing, involving two sub-categories of primary and secondary DHs.

A further indication of the complexity is that there are now five separate categories of consent in the CDR Rules relating to consent for collection, use, disclosure, direct marketing and de-identification. [17] Many of the recommendations of PIA Update 2[18] related to the complexity of the consent options in the CDR regime, but the ACCC's response[19] effectively rejected any simplification.

The PIA reports have identified the complexity of the CDR regime as a primary risk. For example the initial assessment states

> *The CDR Act, together with its interaction with the Open Banking Designation, the Draft Rules, and the Draft Data Standards, is very complex. We suspect that it may be difficult for some CDR Consumers, Data Holders and Accredited Data Recipients to comprehend.*[20]

Consequently

> *the complexity of the CDR legislative framework, [means] that CDR Participants may not understand their rights and obligations under the CDR regime, including:*
>
> *(a) when CDR Data is governed by the APPs and/or the Privacy Safeguards;*
>
> *(b) their obligations as a particular type of CDR Participant; and*
>
> *(c) how the APPs and the Privacy Safeguards apply to them and the data that they hold, including interactions between the APPs and the Privacy Safeguards;*
>
> *[and]*
>
> *CDR Consumers, particularly vulnerable consumers, [may] not [understand] how their CDR Data will be managed under the CDR regime, or the implications of providing consent, authorisation or other agreement;*

Complexity and confusion are raised in every subsequent PIA. Notably PIA update 2 of the PIA which stated that

---

[17] Competition and Consumer (Consumer Data Right) Rules 2020 (Current version), Rule 1.10A.

[18] Australian Competition and Consumer Commission, Consumer Data Right Regime, Update 2 to Privacy Impact Assessment Analysis as at 29 September 2020 Report finalised on 8 February 2021https://www.accc.gov.au/system/files/CDR%20v2%20Rules%20%E2%80%93%20Update%202%20to%20Privacy%20Impact%20Assessment.pdf

[19] Consumer Data Right Rules Update 2 to Privacy Impact Assessment Agency response February 2021, https://www.accc.gov.au/system/files/Attachment%20B%20-%20ACCC%20response%20to%20update%202%20to%20Privacy%20Impact%20Assessment.pdf

[20] Page 44, Department of the Treasury, Consumer Data Right Regime, [Analysis as at 23 September 2019] https://treasury.gov.au/sites/default/files/2019-12/p2019-41016_PIA_final.pdf

> *"the overall complexity of the proposed amendments, … will significantly add to the already complicated legislative framework underpinning the CDR"*[21]

And in update 3:

> *We consider that the complexity of the framework underpinning the CDR regime means that entities participating in the CDR regime (such as Data Holders, Accredited Persons and Accredited Data Recipients) and CDR Consumers may not understand, or take steps to action, their obligations or rights under the legislative framework*[22]

Although some of the PIA recommended mitigants have been acted on, others have not, resulting in significant continuing risks confronting consumers, despite the high sensitivity of much of the data.

While a CDR consumer might not need to understand all of these complexities in the CDR ecosystem, the detailed disclosure/consent requirements mean that some at least need to be explained. It is legitimate to ask the question whether it is practical and realistic to expect CDR consumers to understand the complex ecosystem which they will be invited to join, to the extent that would be necessary for them to make informed decisions. It seems doubtful that many consumers will be at all interested in the machinery underlying any new services such as supplier comparison or switching sites. If they desire these services, there is a significant risk they will just accept whatever T&Cs, including privacy policies, are imposed.

Therein lies the risk for consumers – that the complexity will lead to them to choose not to engage with the consent system enough to truly know and understand what they are consenting to. CDR consent in this context essentially falls back to the much maligned tick and flick settings that the CDR was meant to resolve.

The CDR over-relies on disclosure as the principle means of consumer protection.

The CDR Privacy Safeguards are based on a "disclosure and consent" model similar to that underpinning the *Privacy Act* but more prescriptive in terms of both the information to be disclosed to consumers and the "granularity" of consent required – both for collection and for specific and distinct uses and disclosures of consumer data.

The underlying premise of the CDR disclosure and consent protections[23] is that if individuals are adequately informed about an organisation's intentions in respect of personal information/data,

---

[21] Consumer Data Right Rules Update 2 to Privacy Impact Assessment Agency response February 2021, https://www.accc.gov.au/system/files/Attachment%20B%20-%20ACCC%20response%20to%20update%202%20to%20Privacy%20Impact%20Assessment.pdf

[22] Department of the Treasury, Consumer Data Right Regime, Update 3 to Privacy Impact Assessment Date of analysis: 17 September 2021 Report finalised on: 29 September 2021 https://treasury.gov.au/sites/default/files/2021-10/p2021-213006-pia-maddocks.pdf

[23] *The disclosure and consent model is implemented in* Privacy Act 1988 *through the interaction of Australian Privacy Principles 1, 5 and 6 (and for certain purposes Australian Privacy Principles Section 7 and 8), and in the CDR, through the same numbered Privacy Safeguards (with an additional Privacy Safeguard 10).*

then they are in a position to be able to give or withhold informed consent for proposed uses and disclosures.

There has been considerable academic argument to the effect that the "disclosure and consent" model cannot be the sole basis for effective privacy protection. Consumer surveys find that people favour "in principle" being given more information and more choice over uses and disclosures of their personal information or data. However, practical experience is that few can be bothered to read privacy notices, statements or policies, and most will simply "tick a box" giving consent to almost anything if that is the simplest and easiest way of obtaining a service they desire.[24]

Default "privacy on" settings, with individuals having to give express affirmative consent for secondary uses and disclosures (opt-in) gives far more control than "opt-out" opportunities. Most people will not take advantage of these, but even "opt-in" is subject to manipulation (or even coercion) if it is the "price" of something that the individual wants. Short term benefits will often be valued more highly than the possibility of long-term detriment, even if the individual can be made aware of privacy risks.

The limitations of the "disclosure and consent" model have been well- documented, including in a joint 2019 report by Australian and Dutch regulators, which characterised disclosure as "necessary" but not "sufficient" and in some cases contributing to consumer harm (ASIC and DAFM, 2019).

In the CDR context, it seems likely that the very elaborate requirements for disclosure and consent, through multiple "consumer dashboards" and referral of consumers to CDR policies (in addition to a separate privacy policy and a range of T&Cs) may be ineffective. They may achieve little practical privacy protection while acting as a barrier to the take-up of CDR both by consumers and by industry principals and intermediaries who the government expects to offer an enhanced range of services. To date, industry entities are finding that design and compliance with processes to participate in CDR are excessively onerous, and consumers are having difficulty understanding industry entities' offerings.

It is not that privacy protections based on the "disclosure and consent" model are unnecessary and should be weakened or even dispensed with. The "disclosure" element is essential as a means of delivering transparency both to consumers and consumer advocacy organisations. The "consent" element is important to the minority of consumers who can cope with the complexity and whose activism plays a role in the protection of all other, less capable and/or less committed consumers.

It is necessary to recognise, however, that the "disclosure and consent" model, in complex circumstances such as CDR, is insufficient to deliver adequate privacy protections. It is essential that appropriate obligations be imposed on service-providers that complement the consent-based approach.

---

[24] Again see CPRC 2020 Data and Technology Consumer Survey – CPRC for insights on consumer engagement.

The CDR regime has incorporated some elements of a regulatory model to protect privacy, in the form of express prohibitions of some data practices, for example some direct marketing using CDR data. However, it is not clear that the pattern and intensity of legal obligations imposed on the many organisations involved in CDR satisfies the requirement of sufficient and suitable protections complementary to disclosure and consent.

We believe that there are ways to move away from this over-reliance – introducing a prohibition on unfair trading practices and a data fiduciary obligation - discussed further below.

Not all government data sets are alike

Financial Rights is supportive in principle of making some government data sets accessible via the CDR where a net public benefit can be demonstrated to clearly outweigh any concerns about privacy, equity and social justice. However, this assessment needs to be made about each data set independently.

Financial Rights recently surveyed consumers in relation to allowing insurers to access certain public databases to assist consumers in complying with their disclosure obligations and avoid having a claim later rejected because they had overlooked an important detail. We found that there was a wide range of comfort levels for different data sets, with over 70% of people being happy with insurer accessing their driving history (demerits, licence cancellations etc.), claims history and vehicle details, but this fell significantly for other more sensitive data types: Criminal records (66%), financial history (53%) and medical records (46%).

There are also valid public policy concerns involved. Insurers can currently request medical or financial records in the process of assessing a claim, but allowing access to large amounts of data in easily machine readable formats could greatly encourage unjustified fishing expeditions looking for reasons to deny claims. Clearly criminal, financial and medical records contain highly sensitive information and have the potential to lead to unfair, and in some cases unlawful, discrimination. A very wide range of data can be useful to all sorts of service provision and decision-making, however that fact alone should not be sufficient to allow it to be shared.

Data must be obtained with consent, and the information along with any relevant insights drawn from it must be shared with the consumer

Information from government databases should be accessed with the consumer's explicit consent. The same information should be shared with the consumer. This data should not simply enter into a black box to be analysed by non-transparent algorithms. The objective of the consumer data right is to put consumers back in the driver's seat and better extract value from their own data, rather than be exploited for it.

In relation to weather related risk and insurance, there are real opportunities for producing better outcomes by giving consumers and their insurers better access to available data. This should not be done in a way that exacerbates existing information asymmetries; where the insurer knows more about the risks that customers face than the customer themselves. Risk mitigation must be a shared exercise and data held in government databases, and the insights insurers draw from it as applicable to a particular customer, should not be withheld from customers on a commercial in confidence basis.

Recommendations

2. Privacy Impact Assessment should be embedded and implemented in the policy development process at an early enough stage to influence the outcome of the CDR design.
3. Consumer testing needs to be significantly expanded to include statistically significant sample numbers and including larger number of consumers experiencing a range of vulnerabilities.
4. Consumer representative organisations need to be appropriately resourced to contribute to the development of the Consumer Data Right.
5. Reliance on disclosure and consent as the primary means of consumer protection needs to be reduced.
6. Access to government databases through the CDR should be approached on a case by case basis, with the benefits and risks carefully assessed in each case
7. Data from government databases must only be accessed with the consent of the relevant consumers (where it pertains to them personally, or details of their particular property) and should also be shared with the consumer, with an explanation of what the information means and how it is going to be used

Question Three Does the current operation of the legislative settings enable the development of CDR-powered products and services to benefit consumers?

In order to promote a safer CDR - we provide the following recommendations:

Privacy Safeguard 3 re: collection of solicited personal information needs a "fair collection" requirement

Privacy Safeguard 3 is more restrictive and seemingly more privacy protective than Australian Privacy Principle 3. However, it could give rise to abuse of the consent provisions, for example, to justify and automate insurers' continual updating of CDR data from a third party source, or a non-bank lenders updating CDR data to identify financial hardship in order to promote and sell higher cost credit to already struggling consumers.

Privacy Safeguard 3 also lacks an explicit "fair collection" requirement, which may encourage unfair practices, for example in the context of claims investigation in insurance, when CDR is applied to the general insurance sector under Open Finance.

Privacy Safeguard 4: Dealing with unsolicited personal information could be bolstered in line with Australian Privacy Principle 4.1 and 4.3

Privacy Safeguard 4 replicates Australian Privacy Principle 4.3, requiring destruction of any CDR data collected "unsolicited" such as inadvertently as per Privacy Safeguard 4(1)). But there is no equivalent in Privacy Safeguard 4 to two other requirements of Australian Privacy Principle 4 – determining if the data could have been collected if it had solicited it as per Australian Privacy Principle 4.1), and applying all of the other relevant safeguards to any

unsolicited CDR data that does not need to be destroyed as per Australian Privacy Principle 4.3. The reason for this omission is not clear, but can be regarded as lessening privacy protection for CDR data.

Privacy Safeguards 6 and 7 re: Use and disclosure needs to include more definitions and remove the "voluntary consumer data" loophole

The CDR regime as currently implemented substitutes Privacy Safeguards 6 and 7 for Australian Privacy Principles 6 and 7. The Privacy Safeguards are more specific than the Australian Privacy Principles, but also less extensive in their coverage. In addition, the effects of Privacy Safeguards are highly dependent on the definitions of key terms. An example is "required consumer data". This is vaguely described in the CDR rules and hence dependent on articulation in Data Standards issued by the DSB. The outcomes could accordingly be improvements to and/or serious reductions in consumer data privacy.

The CDR regime also features a designed-in loophole in the form of "voluntary consumer data", which in CDR-Banking appears to be undefined, and uncontrolled. Moreover, the consent arrangements under CDR are complex and provide many opportunities for the abuse of anything that can be represented to be "voluntary consumer data".

Particularly in view of the continual ratcheting-down of consumer protections evident since late 2020 we remain concerned about the likelihood that the CDR in practice could further weaken already inadequate protections in relation to the use and disclosure of CDR data.

Privacy Safeguard 11 – Quality of CDR Data needs to be amended to apply to collection or use, and introduce the element of relevance in line with Australian Privacy Principle 10.2

In the CDR regime as currently implemented for banking, Privacy Safeguard 11 imposes some of the data quality obligations from Australian Privacy Principle 10 on DHs as per PS11(1) and on ADRs as in Privacy Safeguard 11(2), but they only apply to the *disclosure* of CDR data, and not to *collection or use*. The quality obligation when disclosing also excludes the Australian Privacy Principle 10.2 requirement for the data to be "relevant". Like Australian Privacy Principle 10, Privacy Safeguard 11 does not include '"not misleading" as a data quality criterion in contrast to the correction obligation under Australian Privacy Principle 13 and Privacy Safeguard 13. Privacy Safeguard 11 also only applies to CDR data when it is being used under the CDR Rules. CDR data may for instance be disclosed under one of the exceptions in Australian Privacy Principle 6, in which case the overlapping quality obligations of Privacy Safeguard 11 do not apply.

Privacy Safeguard 13 re: Correction of personal information needs to be strengthened to require corrections irrespective of how a party becomes aware and enable consumer challenges to refusals

Privacy Safeguard 13 is substituted for Australian Privacy Principle 13 in respect of correction rights and obligations. It is, however, a more limited provision. For example, it lacks a general obligation to make corrections irrespective of how the DH becomes aware of a data quality problem. There is also no provision that enables an individual to challenge a refusal.

Establish a set of consumer-centric success metrics

There is currently no clear measure for what a successful CDR regime looks like. The only measures that seem to be of relevance so far have been the number of parties accredited.

This in no way measures whether there are good outcomes for consumers in their ability to access, control and share their own data, whether the use cases developed are fair and useful, whether consumer's data has been handled safely and securely or consumers lives have been improved by the introduction of the CDR.

We support the CPRC's view that the following success metrics be introduced to ensure that the CDR meets its objects:

- ***Consumer wellbeing***
    - *Ability to secure products and services that genuinely improve their lives without compromising data protection.*
    - *Extent to which consumers are reporting that they are better-off as a direct result of the protections offered through the regime.*
    - *Identification of real-life, specific use cases that are relatable and show a direct consumer benefit that's measurable.*
- ***Empowerment and choice***
    - *Extent to which consumers clearly comprehend the information and adequately understand the journey map of their data.*
    - *Ability to offer genuine choice to consumers on products and services, where a superior product/service is not offered at the expense of weakened protection measures for consumer data.*
    - *Extent to which consumers are reporting that they feel they are in genuine control of their data and that the infrastructure is set up in a way to ensure this at all times.*
    - *Extent of products and services that are accessible and inclusive across the customer base.*
- ***Safety and security***
    - *Ability to protect consumers against data breaches, scams and fraud.*
    - *Implementation of a dispute resolution scheme with an appointment of a Digital Ombudsman.*
    - *Capacity and capability to provide a clear pathway for consumers to notify issues and disputes and have those effectively resolved without placing significant onus on the consumer.*
    - *Ability to effectively audit and enforce the framework to identify rogue entities and make them accountable.*
- ***Building trust***
    - *Extent to which consumers feel they can trust those participating in or linked with others participating in the regime.*

- *Extent of open and transparent reporting of the regime.*
- *Identification of real-life, specific use cases that are relatable and show a direct impact on trust that's measurable.*

Conduct a cost-benefit analysis identifying direct benefits to consumers and introduce an audit and enforcement program

We also support the CPRC's recommendation that a cost-benefit analysis be undertaken to identify the value that economy-wide regime will bring and to whom will it benefit the most – – consumers, or entities with a commercial interest in gathering the data. Furthermore, we support the CPRC's call for a process to be put in place so the regime can be audited and enforced. It is remains unclear how the regulator for example will ensure that data that has been shared is being used by entities in line with the consent that has been provided by the consumers. Regulators need to be proactive and sophisticated to identify harm rather than allow consumer harm to occur and react to complaints. The onus needs to shift away from the consumer and on to regulators to appropriately monitor and enforce the requirements of the regime.

Reverse decisions taken regarding consent and disclosure matters that are unsafe for consumers

The CDR needs to improve consent processes to ensure there is less reliance on mere disclosure and placing the entire onus on the consumer to engage, comprehend and apply all the risks. This includes:

- revert back to an opt-in consent model for jointly held accounts to prevent economic abuse; and
- decrease the complexity of the consent regime with its multiple forms of consent and multiple dashboards;
- require "trusted advisers" to be accredited and agreeing to meet the requirements of the *Privacy Act* in line with the recommendations of the PIA.

These and other legislative changes are discussed further under Questions 4 and 5.

Question Four Could the CDR legislative framework be revised to facilitate direct to consumer data sharing opportunities and address potential risks?

Prioritising the safety and security interests of consumers will assist in developing the appropriate means of direct to consumer data sharing. Doing so would ensure that greater consideration be given to reforms that will solve the problems related to privacy, security and regulatory arbitrage. These include:

Ban screen-scraping and other unsafe data access, transfer and handling technologies as has occurred in the UK and Europe

The CDR legislation does not ban screen scraping and other technologies. Without a ban, there has been very little incentive for businesses to become accredited CDR participants. The higher regulatory hurdles act as disincentive to these businesses from joining in what is meant to be a safer, more reliable and efficient data handling system.

Financially vulnerable people too will continue to be harmed when engaging with the CDR avoidant sector when they seek access to credit, and not concern themselves with the nuances of privacy protections to do so.

Introduce an offence for firms to use data obtained via the CDR without accreditation

The object of the CDR legislation is to ensure consumers can share with accredited parties. This can be guaranteed by prohibiting any firm without accreditation from using information obtained via the CDR.

This would require removing the trusted adviser category, and introducing a more streamlined tiered accreditation system or even consideration of a licencing regime.

Expand the consumer protections and safeguards required under the CDR to the entire economy via reforms to the *Privacy Act*

Many of the concerns with sharing data direct to consumers lies in the fact that the information may ultimately be used by non-accredited parties who are not subject to the requirements of the *Privacy Act*, the improved Privacy Safeguards, and the improved consumer protections afforded those who wish to use this data.

The current review of the *Privacy Act* provides a significant opportunity to lift standards and consumer protections across the economy that would somewhat ameliorate the harms that arise if data is misused, breached, or mishandled.

Question Five Are further legislative changes required to support the policy aims of CDR and the delivery of its functions?

Introduce an unfair trading practices prohibition to the Australian Consumer Law (ACL)

In its Digital Platforms Inquiry report the ACCC has recommended a prohibition on certain unfair trading practices. As identified by the ACCC, harmful practices relating to data collection (including location tracking, online tracking for targeted advertising purposes, concealed data practices, the disclosure of data to third parties, dark patterns, online scams, harmful apps, etc.) are increasingly common.

An unfair trading practices prohibition would eliminate deliberate predatory practices aimed at targeting consumers with sales approaches when they are vulnerable. A good example of this is problematic business models in the non-bank lending sector that target and exploit those consumers experiencing financial hardship.

If Australians are to trust digital products, services and their providers (both inside and outside the scope of the CDR) it is critical that they have the confidence that they will not have their vulnerabilities exploited or be at risk of significant detriment.

An unfair trading prohibition would provide this confidence.

Introduce a data fiduciary obligation

International regulators in the US and EU are currently examining ways to regulate the handling of data that avoids overreliance on consent, notice and disclosure.

A data fiduciary standard is one way to move on from this over-reliance by ensuring that those who hold data need to put the consumer's well-being first.[25]

Fiduciary obligations commonly arise in situations where trust is required between two parties – particularly where one party (a consumer) is dependent on the other (a company or service provider) to perform a service that can only be completed if they are trusted to do so. In this context, the company/fiduciary must uphold a series of duties to its consumers including variously a best interest's duty, a duty of care, and a duty of confidentiality.

Data holders should take on fiduciary responsibilities with respect to the data in similar ways to doctors, lawyers, accountants and other professionals. Like these professions, CDR participants are seeking to entice people to use their platforms and tools and hand over their private information by presenting themselves as trustworthy. While the disclosure of information may be intended to better provide services to patients, clients and users, the information asymmetry and power imbalance in these relationships can be exercised to their detriment.

In applying this concept to companies handling personal data, consumers would then have confidence that their interests are looked after even when consumers "don't understand the technology, the legal terms they are agreeing to, or the full consequences or risks of their actions."[26]

This approach shifts the onus away from consumers of having the burden of having to trust companies to do the right thing with their data, as trust would be automatically inferred via the fiduciary duty requirements.

A duty of care would impose a legal obligation on a company to adhere to a reasonable standard of care while performing any acts that could foreseeably harm the consumer.

Data holders would be obligated to act in the best interests of people exposing their data and online experiences and be prohibited from designing tools and processing data that conflicts with the trusting parties' best interests.

---

[25] Balkin, Jack The Fiduciary Model of Privacy, Harvard Law Review Forum, Vol. 134, No. 1 (November 2020) https://harvardlawreview.org/wp-content/uploads/2020/10/134-Harv.-L.-Rev.-F.-11.pdf

[26] Richards, Neil M and Harzog, Woodrow, *A Duty of Loyalty for Privacy Law*, 99 Washington University Law Review 961 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217

The FinTech sector may argue that applying a fiduciary standard to their data holding would stifle innovation and place "boundaries on a company's otherwise limitless power over users' data." In fact, adopting a fiduciary model would "foster innovation by protecting users whose personal information is necessary to grow and innovate."[27]

Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact Drew MacRae, Senior Policy Officer, Financial Rights on (02) 8204 1386 or at drew.macrae@financialrights.org.au

Kind Regards,

Karen Cox
Chief Executive Officer
Financial Rights Legal Centre

[27] Isabelle Guevara, Data Fiduciaries And Privacy Protection In The Digital Age, August 27, 2021https://www.cba.org/Sections/Privacy-and-Access/Resources/Resources/2021/PrivacyEssayWinner2021#_edn24