Consumer Policy Research Centre

Level 14, 10-16 Queen Street, Melbourne, Victoria 3000

ABN 23 100 188 752 T 03 9639 7600 W cprc.org.au

5 November 2020

By email: ACCC-CDR@accc.gov.au [*requested subject line:* Rules expansion]

Submission by the Consumer Policy Research Centre (CPRC) to the Australian Competition and Consumer Commission: *CDR rules expansion amendments Consultation Paper*

Thank you for the opportunity to respond to proposed changes to the *Competition and Consumer (Consumer Data Right) Rules*.

CPRC is an independent body focused on evidence-based pathways to fair markets for all consumers. We conduct cross-sector research with a focus on essential services, online marketplaces, consumer decision-making, and consumer data. We work collaboratively with academia, industry, government, and the community sector to improve consumer wellbeing by informing policy reform and building capability in practice. Our submissions to earlier Consumer Data Right (CDR) consultations are listed as Appendix 1, we attach these as many of the issues covered in this submission have consistently been raised by CPRC over the past three years.

This response outlines our key concerns regarding consequences of the proposed Rules changes and offers specific suggestions where different approaches may produce better results for consumers. We emphasise that the success of CDR must be measured in terms of consumer outcomes – the extent to which consumers receive: higher quality, or more competitively priced products and services; the value from their data and personal information; and more genuine control over their CDR data. Short-sighted approaches to assessing the success of the scheme by measuring the number of accredited recipients participating fails to put consumers first. A weaker CDR protection regime could enable a large amount of participants, but can also threaten information security, erode consumer trust and allow the value of consumer data to be extracted by industry at ever greater rates, rather than accruing with consumers themselves.

We continue to underscore that this is particularly the case in Australia relative to other schemes such as Open Banking in the UK, where GDPR runs in parallel. Australia, however, has a significantly outdated Privacy Act and consumer protection regime that has not kept pace with technological advancements in the digital age. The ACCC's Digital Platforms Inquiry has drawn similar conclusions, finding that "to enable consumers to make informed and genuine choices, to increase the accountability of entities handling user data, and to provide the ability for consumers to exercise some control over their user data [the] ACCC considers that the most efficient way to make these changes is to amend the existing privacy law and extend protections under consumer law"[1].

Our submission begins with general remarks on the Rules Expansion. Detailed comments in relation to specific proposals follow from page 7.

[1] Australian Competition and Consumer Commission (2019) *Digital Platforms Inquiry: Final* Report, p23.

Consumer Policy Research Centre

Level 14, 10-16 Queen Street, Melbourne, Victoria 3000

ABN 23 100 188 752 T 03 9639 7600 W cprc.org.au

1. General remarks

Economy wide protections

CDR is an ambitious reform that needs to work in complement with other frameworks and with the support of economy wide consumer protections to succeed. Our submissions to consultations in relation to CDR and other digital and data policy reforms in recent years have repeatedly recommended that broad consumer protections are needed to address systemic weaknesses, rather than expecting bespoke and piecemeal legislative approaches to effectively carry this weight. This reflects the inability of regulators and policymakers alike to forecast (and effectively address) the reach of AI and data-driven technological advancements. Data-driven technologies and products and services are not being deployed within a single sector or regulatory regime, in most cases data is being combined across sectors. Without an effective, reliable consumer protection framework across Australia acting as a safety net for the CDR regime and data that may be transferred out of it, we are concerned that there in effect will be a 'race to the bottom' on CDR Rules and Standards as industry increasingly points to the more 'cost effective' regime they currently operate in which can only be described as a regulatory and policy void which is posing significant risks to Australian consumers.

We continue to stress the need for an Unfair Trading Prohibition and a General Safety Provision to be introduced to the Australian Consumer Law, as well as reform of the Privacy Act to give Australian consumers more robust protection when living online[2].

Without effective economy wide safeguards, it becomes incumbent on CDR to provide more specific protections for consumers. The result is increasing detail and complexity being added into the scheme to enact consumer safeguards that should reside in wider consumer protection frameworks. This represents a real threat to the uptake, operation, and sustainability of the scheme, making CDR increasingly difficult for consumers to understand at the same time as it adds intricacy to industry and regulatory responsibilities of participation.

We are concerned that practical effects of failure to frame CDR reforms as part of a larger ecosystem of digital governance in Australia are reflected in the repeated arguments made by some parts of industry who argue that the CDR regime adds burdensome costs (and protections) relative to their business models. The response appears to be a move toward weakening CDR rather than pushing to strengthen overall safety of digital markets for consumers. This fails to recognise that consumer and privacy advocates have long raised serious concerns about current BAU data activities of Australian businesses - many classified as small businesses (including fintechs and other potential CDR participants) for example, do not currently face any Privacy Act obligations at all. This jeopardises one of the key rationales for CDR's existence: to establish a robust and trustworthy mechanism by which consumers can give clear and traceable consent to transact their consumer data.

[2] Priority areas for privacy reforms previously highlighted by CPRC (which we note are within the Terms of Reference of the recently launched Privacy Act Review) include: a) Updating the definition of personal information to include technical data and any other identifiers; b) Introducing direct rights of action for individuals; and c) Introducing a statutory tort for serious invasions of the Privacy Act. See: CPRC (2019) Submission to Australian Treasury consultation on ACCC Digital Platforms Inquiry Final Report, pp. 17-18.

The expansion of the CDR ecosystem through these Rules changes, including bringing disclosure of CDR data to non-accredited parties into scope, heightens the urgency for stronger general economy wide protections relating to fairness, safety, and privacy for consumers. Ideally, broad protections would precede any implementation of Rules changes to expand the (still untested) baseline CDR into areas that significantly add to risk of consumer harm or exploitation[3]. Strengthening economy wide consumer protections in relation to safety, fairness and privacy will help ensure Australian consumers seeking to benefit from CDR are not inhibited by analogue era laws and regulations that do not provide effective protection or deterrence against problematic data practices and business conduct in digital marketplaces, issues that the ACCC has already clearly identified in its Digital Platform Inquiry[4].

Market stewardship

While we do not object to the notion of tiered accreditation in principle, we note that the models being proposed here come with a significant loosening of regulatory oversight. The consultation paper proposes three new accreditation tiers, supplementing the more rigorously monitored 'unrestricted' CDR accreditation. The new tiers rely heavily on "self-assessment and attestation", without corresponding audit and compliance requirements having been clearly defined[5]. We would urge careful consideration of the extent to which such heavy reliance on CDR participants to self-regulate can deliver on the goals for a safe, trusted, and trustworthy CDR.

Proposals aiming to lower entry barriers and compliance costs for business participation in CDR require a clearly articulated plan for monitoring accountability if they are to avoid incurring greater financial and human costs in the future. To preserve the credibility of CDR as deserving of consumer trust, something which the ACCC has articulated as "pivotal" to CDR[6], such aims cannot come at the expense of transparency for consumers and strong market stewardship. The documented track record of Australian markets targeted for CDR's initial roll out demonstrate how easily consumer protection, healthy competition, and sustainable regulatory frameworks are compromised by ill thought out self-regulation[7].

---

[3] For example: disclosure of CDR data to unaccredited parties; unrestrained disclosure of CDR insights; and increased capacity for recipients of CDR data to undertake data profiling (including under the guise of research use cases) and direct marketing. Specific implications of these proposals are discussed in more detail elsewhere in this submission.

[4] Australian Competition and Consumer Commission (2019) *Digital Platforms Inquiry: Final Report* (Chapter 7).

[5] For example, in describing the proposed restricted accreditation tier, the discussion paper states: "The ACCC anticipates that a targeted compliance and audit program for persons accredited to the restricted level would be developed by the ACCC and OAIC as part of their general compliance activities" (p18).

[6] 'Tackling market power in the COVID-19 era'. Speech by ACCC Chair Rod Sims to the National Press Club, 21 October 2020. https://www.accc.gov.au/speech/tackling-market-power-in-the-covid-19-era

[7] For example, we note evidence contained in the Hayne *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* (2019); the Thwaites *Independent Review of the Electricity & Gas Retail Markets in Victoria* (2017); and the public submission made by Financial Rights Legal Centre and Consumer Action Legal Centre to the Senate Select Committee on Financial Technology and Regulatory Technology (2019). On the concept of market stewardship, see CPRC's recent report *The experiences of older consumers: towards markets that work for people* (2020).

The speed and direction of changes suggested by this CDR Rules Expansion take regime in a direction where rights held by consumers in relation to their data are diminished in favour of rights assigned to entities seeking to make use of consumers' data. We see in these amendments a broadening of permitted uses and disclosures of CDR data at the same time as transparency and safeguards for consumers are being narrowed under CDR Rules, and in other regulation that CDR will intersect with[8].

A consumer-centric CDR has been articulated as a clear goal of the reform from the outset[9]. While we acknowledge that the definition of 'consumer' for CDR purposes is wider than individuals, the data rights of individual consumers are integral to how CDR has been conceived and promoted to date, and should remain at the heart of the Consumer Data Right. Robust consumer protections for Australians across all walks of life must not be removed from the fabric of CDR.

Transparency for consumers

We maintain that consumer choices, agency and protections must not be compromised by a roll back of consumers' visibility over disclosure and use of CDR data. The proposed Rules changes risk transparency for consumers being decreased, including reductions to the simplicity and clarity of managing consent due to effects of the proposed separation of collection, use, and disclosure consents. This separation is posed as offering consumers more control, however we believe the outcomes in practice will be: higher cognitive load for consumers; increased scope for dark patterns and nudges being used to steer consumer choices regarding use and disclosure of CDR data; and a greater level confusion for consumers over what they are consenting to.

Despite the ACCC's decision to reject the recommendation of Update 1 to the PIA in relation to consumer visibility over CAP arrangements, on the basis that they consider information supplied to the consumer as part of an ADR's generic CDR policy is a sufficient extent of disclosure regarding use of outsourced service providers to collect or process consumer data[10], we continue to support Recommendation 4 of the PIA. We firmly believe that consumers should be notified of the substance as well as the fact of CAP arrangements (ie, consumers should have visibility over who and how their consent gives permission for parties to handle their data under CDR arrangements), and that this information should be accessible via the consumer dashboards provided by data holders, as well as data recipients. How this information can be best presented for clear consumer comprehension should continue to be a subject for CX research, testing, and monitoring within the CDR regime.

---

[8] For instance, consumer groups have warned the intended rollback of Responsible Lending Obligations under proposed changes to the National Consumer Credit Protection Act is likely to lead to higher levels of household debt overall, and in particular to increase the incidence of financial hardship due to people taking on debt they cannot afford (see, for example: https://www.abc.net.au/news/2020-09-25/government-responsible-lending-changes-home-loan-credit-cards/12702260).

[9] "The Consumer Data Right will be implemented according to four key principles: [1] The Consumer Data Right should be consumer focused. It should be for the consumer, be about the consumer, and be seen from the consumer's perspective." The Treasury (2019), *Consumer Data Right Overview*, Commonwealth of Australia.

[10] *Consumer Data Right Rules - Update 1 to Privacy Impact Assessment: Agency response* (October 2020); Recommendation 4.

Our recent research into CDR[11] suggests the diverse needs and capabilities of consumers are not being taken into account to create a sufficiently accessible CDR regime, and we propose more regulatory engagement and guidance is needed on what good and bad consumer experiences look like across the spectrum of Australian society. Before moving ahead with proposals regarding separation and amendment of consent in CDR, we advise further CX research on consumer expectations and comprehension of consent (extending on initial work undertaken by the Data Standards Body). This should include the development of indicators for meaningful consent; and deeper investigation of consumer expectations for the representation of consents on consumer dashboards – including the implications of, and tolerances for, discrepancies between CDR information conveyed on dashboards provided by data holders and accredited persons.

It is particularly concerning to us that consumer consent across collection, use, and disclosure will not be able to be withdrawn unilaterally from the data holder consumer dashboard (which, for banking CDR data at least, is likely to be the most familiar and convenient interface for consumers seeking to engage with their CDR consents). We realise that the Rules have always mandated consumers' withdrawal of consent to occur through the accredited person's consumer dashboard (because the consent agreement is between the consumer and the accredited party). Nonetheless, we believe an amendment to the Rules that would support the data holder consumer dashboard functioning as the mechanism through which a consumer's direction to withdraw consent could be lodged and communicated would be beneficial.

As well, in the case of joint accounts, we note the loss of account holder B's visibility over the current state of active CDR consents in situations where such consent is amended by account holder A. In addition to removing awareness over how their data is being handled, this effectively invalidates the right of account holder B to withdraw authorisation for amended permissions in relation to data usage and disclosures that they do not consent to (for the simple reason that they are not aware this consent has been given). Our view is that these are not acceptable consumer trade-offs. We reject the notion that providing better granularity of consent requires removing consumer visibility and control over elements of that consent.

Consumer choice and safety

We consider there is significant potential for consumer harms (such as increased profiling, predatory pricing, and barriers to seeking redress) arising from proposed amendments that loosen protections against direct marketing and which expand permitted uses of CDR to include disclosure and sale of derived insights, commercial research by data recipients, and greater allowances for on-selling of CDR data. CPRC strongly recommends that the amendments to the Rules proposed at 7.5(1)(aa) and 7.5(3)(a)(iv) should be struck out, along with any relevant enabling clauses.

We would encourage the ACCC to further explore and investigate the nature of the derived data and insights that industry would be enabled to on-sell. Banking data is highly sensitive, potentially containing information and facilitating insights about personal matters including health (alcohol,

[11] See: *Stepping towards trust – Consumer Experience, Consumer Data Standards and the Consumer Data Right* (released September 2020) and *Joint Accounts and the Consumer Data Right: Perspectives from Community Organisations and Consumer Advocacy* (forthcoming, pending public release).

food, gym membership payments, sensitive medical appointments and treatments), whether consumers are recipients of government payments, family and friends (as well as businesses) who are regularly transacted with, and political affiliations through event attendance / donations. We continue to raise the high probability that these are the sorts of insights that can and will be extracted and on-sold as a result of this proposal being enabled under the CDR regime as currently drafted in the Rules amendments.

As well, although we support the right of consumers to choose to access and share their CDR data as they see fit, we cannot endorse the proposal to permit disclosure of CDR data to unaccredited third parties in its current form. Not only does this proposal place data outside protections of the CDR but it also requires such disclosures to be mediated by an ADR who is permitted to charge for the service. As such, it indicates similar outcomes and risks as could be achieved by activating CDR's provision for direct to consumer data sharing (ie, for consumers to request their CDR data directly from data holders and share it with a trusted party) - but with less agency for consumers, and no additional benefit beyond providing ADRs opportunity to monetise a service that might otherwise be a free right for consumers. We emphasise that we do not think the existing environment, in which such data sharing would often fall entirely outside Privacy Act protections, is robust enough to support either direct consumer access or the mediated disclosure to trusted advisors ("TA disclosure consent") proposed in the proposed amendments.

Vulnerability and inclusion

More needs to be done in the Rules to ensure CDR is an inclusive reform underpinned by a coherent and comprehensive strategy for supporting consumers who are experiencing vulnerability. Our 2019 report for the Australian Energy Regulator (AER) underscores how vulnerability affects the choices and interactions consumers have with markets.[12] It highlights areas where markets and providers may exacerbate harms, and pinpoints why a nuanced understanding of real-life experiences is necessary to creating inclusive market reforms.

We note the proposed Rules changes that effectively allow data holders to treat joint accounts flagged for abuse as if they were not joint accounts, to better protect the account holder experiencing abuse. We support this safeguard as an important and valuable protection; however, we also feel it is important to also acknowledge its limitations. These are: 1) reliance on the ability of vulnerable consumers to confirm or self-disclose abuse (which is not always possible, particularly in relationships characterised by coercive control or violence); 2) reliance on there being sufficient cultural and technical capacity within organisations to recognise and accommodate such disclosures and to apply protocol for implementation of associated safeguards; and 3) practical implementation being contingent on technical provisions that are declared to be optional rather than mandatory (ie, co-approval on joint accounts).

We believe CDR should continue to iterate and improve the experience and protections it will offer victim-survivors of domestic violence, and encourage the ACCC and banks to work with family

[12] Emma O'Neill (2019), *Exploring regulatory approaches to consumer vulnerability – a report for the Australian Energy Regulator*, Melbourne: CPRC. We also point to the example set by Open Banking in the UK in exploring market impacts for a range of consumers: Faith Reynolds, et al (2019) *Consumer Priorities for Open Banking*.

violence specialists to design more effective ways to enable financial counsellors and support workers to advocate on behalf of clients and access CDR data on their behalf.

More broadly, we share concerns raised by consumer advocates that increased availability of consumer data through the CDR, if not well regulated, is likely to see increased competition for 'high value' customers at the expense of vulnerable consumers, and we emphasise the importance of distributional impacts of this kind being monitored by government, as well as the need for CDR policymakers to develop a clear measurement framework for consumer outcomes[13].

2. Comments regarding specific proposals and amendments contained in the CDR Rules Expansion consultation

Introduce new accreditation levels

Our key concern with the three proposed accreditation models is the emphasis on "attestation and self-assessment" as the method of maintaining accreditation. The discussion paper states this will be "complemented by a targeted audit and compliance program" (p10), however articulation of what such oversight will consist of is not included as part of the proposal, with the consultation paper noting these requirements are to be developed at a future time[14]. Our view is that this information should be clear before the tiered accreditation proposals are decided on: it is not possible to fully assess the sufficiency of consumer protections in relation to proposed accreditation levels which are reliant on self-regulation[15] in the absence of a framework for how compliance will be monitored.

We also challenge the assertion presented in the executive summary of the consultation paper that "CDR participants can appropriately manage risk and liability through commercial arrangements" (p4). Although this may be true at the level of capital risk, the findings of substantial inquiries such as the Haynes Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry indicate it does not hold true for risk outcomes faced by consumers. Past behaviours demonstrated in these sectors (and others) does not warrant implicit trust of consumers, or engender confidence for self-regulated aspects of CDR.

As well, we are interested to better understand how consumers will be alerted to the different levels of accreditation operating within the regime, and how they will be made aware of the accreditation level held by the various data recipients they might enter into agreements with. We consider this is necessary information for consumers to be able to assess their comfort with risk, and to make informed choices and consents about how they share data, especially in an environment where

[13] CPRC has sketched out a foundation for this work in a recent report for the Data Standards Body that documents key consumer needs from CDR data sharing and high level indicators for each of these criteria, against which meaningful and quantifiable measures might be articulated. Refer Section 3 of *Stepping towards trust – Consumer Experience, Consumer Data Standards and the Consumer Data Right*.

[14] See note 5.

[15] For example, the proposed amendment specifying "criteria for affiliate accreditation" (Rules 5.5A) requires only that the applicant has a sponsor and that the sponsor certifies the applicant meet the criterion specified in Rule 5.5.

other proposed reforms, such as the proposed roll back of Responsible Lending Obligations, are putting more responsibility for risk onto consumers.

We note the proposal that CDR data types subject to access under a Limited data restriction would be defined for each sector with industry consultation does not include commensurate provision for consumer consultation. Consumer input is equally important for determining sensitivity thresholds for consumer data types and consultation processes must reflect this.

We also have concerns that proposed models for accreditation may have the effect of making it more difficult for consumers to distinguish between their consents. For example, in the case of data enclave accreditation, we envisage scenarios where a data holder's consumer dashboard may not show information that is meaningful to the consumer because the consumer understands their consent as being linked to the principal not the provider, whereas the dashboard is required to show only provider information.[16]

Disclosure to trusted third parties

We are opposed to the disclosure CDR data to unaccredited parties (aka 'trusted advisors') as it is framed in the proposed Rules expansion.

We reiterate our earlier comments that this proposal not only places data outside protections of the CDR but is also limiting consumer agency by requiring such disclosures to be mediated by an ADR. The risks of movement of data outside the CDR system are not being mitigated by this proposal in any meaningful way (as is highlighted in Update 2 to the PIA)[17], and there is no obligation on non-accredited parties to delete data in accordance with any election made by the consumer (as this election only applies to CDR data held by an accredited person). We suggest a better outcome for consumers would be to adjust this proposal to instead carefully scope and implement direct to consumer CDR data sharing.

We emphasise that additional consumer safeguards, such as the economy wide reforms we recommend at page 4 of this submission, are required for direct consumer access to occur in a safe environment, and to mitigate increased risks to consumers of CDR data being misused or mishandled:

- by commercial entities who are not accredited and bound by CDR rules and safeguards, who may have requested the data direct from consumer as a means of bypassing CDR regulation;[18]

[16] We note proposed rules changes to support clarity for consumers in similar situations where a parent company may be the accredited party (per use case described on p47 of the consultation paper), and suggest measures would also be required to ensure a data holder's consumer dashboard includes metadata for principal (not just provider) in data enclave arrangements. We note as well that changes to Rule 7.4 require the fact, but not the substance, of CAP arrangements to be disclosed on an ADR's consumer dashboard.

[17] Maddocks (2020) *Australian Competition and Consumer Commission Consumer Data Right Regime - Update 2 to Privacy Impact Assessment: Stakeholder Consultation Document; Analysis as at 29 September 2020*; p65 (analysis of Risk 23).

[18] We note that in relation to commercial entities, allowing data to be disclosed to non-accredited entities may act as a disincentive for businesses to participate in the CDR framework if they can access the same data through alternative pathways without being subject to CDR requirements.

- by non-commercial entities who are operating in the consumer interest but who may not have relevant security protocol for the management or storage of data; or
- by the individuals themselves (through lack of data security, or other reasons, potentially including malicious disclosure of sensitive data relating to joint accounts as a form of abuse).

In relation to use of CDR data by non-commercial entities operating in the consumer interest (such as financial counsellors, or community legal services) CPRC sees greater value in exploring an ADR exemption framework that could allow specified organisations to request data on a consumers behalf and to use the CDR data only for a specific (and auditable) purpose with appropriate privacy protections put in place as approved by the ACCC and OAIC. Such requirements could also provide guidance for use of CDR data by organisations where it is provided by a consumer following Direct Consumer access.

Our recommendation is that amendments allowing "TA disclosure consent" (as defined in Rules 1.10A) should not proceed. However, if this proposal were to be progressed, there must be a requirement added for any associated fees charged by ADRs to be waived in situations where consumers are seeking the data to be provided to pro bono or community legal services (and other similar, non-commercial services). We also note that making disclosure to third parties contingent on specific professional affiliations may inadvertently cut out opportunities for service provision to consumers experiencing vulnerability – for example services that function as a first step or referral pathway to provide consumers with advice about their *options* without necessarily providing a legal opinion or financial advice. If the proposal is to be implemented, stronger consideration must be given to how it can be framed in a way that provides meaningful benefit for vulnerable consumers.

Disclosure of insights

We are strongly opposed to the expansion of the CDR Rules to include disclosure of insights derived from CDR data to any party. CPRC recommends that the proposed expansion to the Rules permitting use of CDR data for the specific purpose of the creation of insights[19] should be struck out, along with any relevant enabling clauses, including those in relation to 'insight disclosure consent'.

We concur with Update 2 to the PIA that there is specific risk to vulnerable consumers associated with this proposal, particularly in circumstances where consumers may not realise the potential negative consequences that could arise as an outcome of providing their Insight Disclosure Consent; or where they may be pressured into providing their Insight Disclosure Consent by a potential provider of goods or services.[20] We also agree that disclosing CDR insights may be more invasive[21] – and potentially more damaging – than raw data. To the risks identified by the PIA in Update 2, we

[19] Rule 7.5(1)(aa)(ii).
[20] Maddocks (2020), p66 (analysis of Risk 24).
[21] Maddocks (2020), p67 (analysis of Risk 25).

would add that CDR insights will be especially dangerous as they are liable to be taken as 'fact', rather than being recognised as the product of opinions embedded in code[22].

Although we do not support inclusion of insight disclosure in the CDR Rules, if this proposal were to be brought into the scope of CDR, it is essential that it include requirements to clearly communicate to consumers what the "insight" and information they are consenting to be disclosed is; what the benefit of the disclosure is for the consumer; and who they are giving consent for it to be disclosed to (ie, a requirement that CDR consumers provide express consent for this, not simply to be informed after the fact)[23]. As well, consumers must have the right to request, at no cost, an exact copy of any insight disclosed under an insight disclosure consent they have given.[24] Without free access to a copy of the insight, a consumer will not be able to challenge its accuracy or seek correction to the insight in matters of dispute resolution or redress.

The two scenarios presented on the following page illustrate examples of areas where we would be seeking clarification of how CDR insight disclosure is intended to work. If insight disclosure could readily lead to the kinds of outcomes described in these scenarios, we emphasise the need for more extensive protections for consumers.

Permitting use of CDR data for research

We are opposed to the use of CDR data for research, as it is framed in the proposed Rules expansion. We can see social value and opportunity in allowing consumers to choose to share their (deidentified) CDR data for public good and non-commercial research purposes[25], but we do not consider the proposed Rules amendments are geared towards 'data for good' initiatives. Rather, the proposed changes appear designed to facilitate CDR data being used by data recipients to undertake market research and build data profiles unrelated to their provision of a specific service to the consumer. These activities run counter to the original principles of CDR.

---

[22] On the propensity for data driven insights to reinforce structural discrimination, see O'Neil, Cathy (2016) *Weapons of Math Destruction* Crown Random House. Algorithms can apply consistency to the production of insights, and they can also produce insights that are consistently wrong.

[23] We see merit in the suggestions posed by the ACCC in Consultation question 19 (but which are not part of the amendments as currently proposed): that consumers might "be able elect to view an insight before they consent for it to be disclosed to a non-accredited person" and that "ADRs be required to provide the option for consumers to view insights via their dashboard". We agree that both requirements would improve transparency for consumers regarding insight disclosure. Expanding on these suggestions we suggest that if insight disclosure is to be allowed, express consent to each insight should be mandatory requirement. We emphasise this should not displace any right to later obtain a copy of the insight as disclosed.

[24] The proposed amendment requiring a data recipient to notify consumers of insight disclosures on the consumer dashboard is not sufficient, as it guarantees the consumer a record of metadata only (we gave company X an insight on date Y based on consent Z). If a consumer is denied access to an essential service – such as rental housing, for example – on the basis of an insight disclosure consent but is not given access to the insight itself they will be limited in their ability to understand or challenge this outcome.

[25] For example, as an evidence base for developing rental protections, energy concessions, or other public policy initiatives; or to build energy usage datasets that can inform clean energy market policy.

SCENARIO 1:

Cal signs up to a budgeting app 'Pebble'.

Cal's impatient to get started, so he ticks all the boxes relating to consent. In doing so, he has provided Pebble with CDR consents to use his data for research and direct marketing, as well as giving them an insight disclosure consent. Pebble collects data about Cal's use of the budgeting tool, showing he usually logs on late at night and is most interested in reviewing the status of his gambling debt, and combines this with CDR data from his credit card showing frequent spending on online gambling sites and cash advances at the casino.

Pebble on-sells insights about the percentage of Cal's income that is spent on gambling to one of the betting companies Cal has an account with. Based on this insight, they begin to target him with new offers as there is no prohibition on companies outside CDR direct marketing based on insights they have purchased. Meanwhile, Pebble begins making direct marketing offers to Cal for a number of personal loan products where they have relationships with the vendor (and take a fee for referral conversions). They justify this direct marketing on the basis that a personal loan will be better for Cal, budget wise, than cash advances with a high interest rate.

Cal takes out a personal loan but also increases his spend on online gambling – the loan is soon exhausted, and Cal now has more debt than when he signed up to Pebble.

SCENARIO 2:

Ngarie is seeking a new residential rental property.

She has found a place she likes and is ready to lodge her rental tenancy application. The property manager informs Ngarie that to complete the process the agency has a policy of confirming rental payment history using 'Verity', a trust scoring service. Ngarie is told that if she wants to apply for this property, she will have to abide by this requirement.

Ngarie isn't 100% comfortable with this, but she really likes the property so she provides a CDR consent to Verity for a one off collection, use, and insight disclosure relating to the transaction account from which her rent was paid by direct debit.

The next day, Ngarie's tenancy application is rejected. She doesn't know if it is because of the insight provided by Verity to the real estate agent, or for another reason. She remembers now that her rent was late one month when a direct debit was dishonoured because all her utility bills are set up for automatic direct debit and she didn't realise the account would be short for the rent. Ngarie asks the property manager if this is the issue, and explains it was a one off. However, the property manager won't provide any further details about Ngarie's application being rejected, and simply says another tenant has been accepted. Next, Ngarie contacts Verity, but they say they are not obliged to tell her what the insight contained.

Now Ngarie is anxious about her ability to secure housing and unclear about what will happen if she applies for another rental property listed by this agency, or with another real estate agent who uses Verity.

The consultation paper explains that "benefit to the consumer [of consenting to research use of CDR data] could be, for example, the ADR paying a fee to the CDR consumer or providing a discount on services provided to the CDR consumer. If the consumer consents to this research use, this would allow the ADR to use the data collected for providing a good or service for other activities such as product development or business development" (p48). We predict significant scope for a provision of this kind to be exploited and we suggest it is highly unlikely that consumers would be compensated a fair market value for their data without an explicit requirement being made for ADRs to do so.

We do concur with the ACCC that it is essential for the use case relating to any research use of CDR data to be clearly articulated to consumers. We also note proposed amendments to the Rules require that when an accredited person is asking a CDR consumer to give consent for this purpose, they must provide a link to the description in the Accredited Data Recipient's CDR Policy which specifies the research to be conducted, and any additional benefit to the CDR Consumer for consenting to the use of their CDR Data. However, we highlight that presenting the relevant detail of consent in this manner could, if not well managed and monitored, run the risk of contravening Rule 4.10(b).[26]

Joint accounts

We support amendments that will require making clear in a Joint Account Management Service (JAMS) that data sharing activity/consent would be seen by the other account holder(s). However, we also wish to amplify a clear message from domestic and family violence services conveyed in our recent research into CDR and joint accounts[27]: this alone does not go far enough in fulfilling a duty of care to people experiencing abuse.[28]

We reiterate our earlier comments that the loss of account holder B's visibility over the current state of active CDR consents (in situations where consent is amended by account holder A) does not sufficiently support consumer transparency and meaningful consent for joint account holders. In addition to removing awareness over how their data is being handled, this situation effectively invalidates the right of account holder B to withdraw authorisation for amended permissions in relation to data usage and disclosures that they do not consent to; for the simple reason that they

[26] Rule 4.10b states that processes for obtaining consent must not include or refer to other documents so as to reduce comprehensibility.

[27] CPRC (2020) *Joint Accounts and the Consumer Data Right: Perspectives from Community Organisations and Consumer Advocacy*. Report produced for the Data Standards Body (pending public release).

[28] For example, in the scenario of a coercive and controlling relationship where abuse is not known to the DH (a bank) the perpetrator of abuse may in fact be in control of the abused party's online banking account, so that they were not be involved in supplying a JAMS approval (despite appearances that they have given valid approval) and did not see the notification. If the victim-survivor subsequently seeks to escape the abusive relationship and build financial recovery using CDR, they may not realise that the other party will be alerted to their CDR activity; which could have serious repercussions to their safety. In other scenarios, such as for energy CDR data, there will be no JAMS through which this information can be conveyed. Accordingly, we advise it is essential for a joint account holder to be notified at the time of making each consent that data sharing activity will by default be seen by the other account holder(s). As the ADR does not have visibility over whether a consent relates to a joint account, this may need to be implemented as a requirement on the DH at the authorisation decision point during the consent flow.

are not aware this consent has been given. Our view is that this is not acceptable, our suggestion to remedy this scenario is given below.

It is proposed that data recipients will be required to notify data holders of amendments to consent to mitigate implications for consumer dashboards going out of synch because of amended consent.[29] We suggest there should also be a requirement for this data to be provided by ADRs in a format that enables it to be easily communicated back to consumers via the data holder dashboard. Where amended consent related to CDR data that is being collected from a joint account, this would enable all account holders to have visibility over the current state of consents.

Amending consent & Separation of consent

We have considerable reservations about the likely implications of separating and amending consent in CDR and the extent to which this may inhibit consumers from being able to easily withdraw consent[30], potentially undermining the fundamental CDR provision that consent should be as easy to withdraw as to give. Although we agree that separating consent for collection, use, and disclosure of CDR data has potential consumer benefit if it results in consumers being able to exercise more specific control over CDR data, we are concerned that in practice the reverse may prove to be true. The types and categories of consent proposed at Rule 1.10A come with an expectation that consumers will be able to differentiate between them (which may not always be the case) and will add complexity and cognitive load to the process of providing, managing, and withdrawing CDR consent. This may be to the detriment of both consumer comprehension and the quality of consent being provided.

We draw attention to page 44 of the Rules Expansion consultation paper which explains: "The ACCC implemented a combined concept of a 'use and collection consent' in the current rules based on earlier consumer experience findings. The ACCC is proposing to move away from this approach with the development of rules that allow for separate consents for collection of CDR data and consents to use CDR data. Re-framing the rules so these consents are separate concepts creates more flexibility for accredited persons and enables more granular consent options". While this may be an issue of expression, we are nonetheless concerned by the suggestion that CX findings about how consumers want to give consent may be so easily set aside to provide greater flexibility for accredited persons. We fear that this is symptomatic of a Rules Expansion which is vastly benefiting data recipients at the expense of known consumer needs and expectations.

Changes to consent processes in CDR should have a primary motivation to help ensure consumers are able to make meaningful choices, express those choices clearly, and manage them easily. For

[29] "Where consumers amend their consent, the proposed rules require the accredited person to notify the data holder, in order for the data holder to invite the consumer to correspondingly amend their authorisation. This ensures the consumer dashboards are synchronised and technical mechanisms prevent the disclosure of CDR data no longer subject to a valid consent." (ACCC CDR Rules Expansion Consultation paper, p42).

[30] As one example, we refer again to the scenario provided in our general remarks: where consumer consent in relation to a single use case and data holder, by being separated into component consents for collection, use, and disclosure, may no longer be able to be withdrawn in a single step from the data holder consumer dashboard. We reiterate our view that, for banking CDR data at least, the DH consumer dashboard is likely to be the most familiar and convenient interface for consumers seeking to engage with their CDR consents.

separation of consent to work effectively as a mechanism to allow consumers more nuanced control over their CDR activity, all consumers whose CDR data is covered by a consent (including joint account holders) must be kept clearly aware of the changed state of amended consents, and consumers should not have to jump through hoops in order to extricate themselves from any consents given under CDR.

We disagree with the position put forward in the consultation paper that it is acceptable for joint account holder B to lose oversight or control over further disclosure of their CDR data by the accredited person: "if joint account holder A provides a consent for an accredited person to disclose their CDR data … joint account holder B will have no transparency or notification of that disclosure" (pp 40-41). Nor do we agree that "technical implementation costs for data holders and accredited persons to implement additional oversight for joint account holder B outweigh the potential benefits, particularly given accredited persons offering 'multi-party centralised dashboards' may competitively fill this gap" (p41). Although competitive providers *may* fill this gap our view is that the Rules *must* require such oversight for joint account holders. Anything less is a clear denial of the fundamental CDR right for consumers to consent to how their data is shared.

Dashboards

Placing consumer dashboards solidly in the competitive space (as is suggested by the remarks at p41 and elsewhere in the consultation paper) – while not inherently a bad thing – will risk leaving vulnerable consumers unable to access a fundamental mechanism for monitoring and managing CDR consents if the shift is not accompanied by mandatory and enforceable obligations on dashboard providers to adhere to accessibility requirements and other CDR CX Standards.

Regardless of whether principal or provider is the accredited party charged with supplying consumer dashboards[31]; here, as in other areas (such as amending consent[32]) we are concerned by the extent to which CDR dashboards provided by data holders and accredited persons may display inconsistent information in relation to the same consent. Discrepancies between consumer dashboards will undermine consumer trust and hamper comprehension, having an adverse impact on consumers' understanding and management of the consents they have given to share CDR data. This is a bad outcome for consumers and underscores the need for ongoing attention to the consumer experience of CDR, particularly where key elements of the regime (such as consumer dashboards) are outsourced to RegTech providers whose first imperative is to their customer, rather than to the CDR consumer.

Any design of consent dashboards should be completed through direct consultation and research with *consumers themselves* to ascertain how they would prefer to access and amend their CDR data, not according to the preferred method for industry.

[31] Rule 7.4 indicates the ADR collecting the CDR data has the responsibility updating the (recipient-side) consumer dashboard accordingly ie, is responsibility of the provider not the principal. However, Consultation question 14 indicates this is under consideration for change: "We consider that in the case of a CAP arrangement, it is appropriate for the principal (having the relationship with the consumer) to be responsible for ensuring that customer-facing aspects of the CDR regime are delivered (for example, dashboards and any customer-facing communications, including in relation to dispute resolution)."

[32] ACCC Rules Expansion Consultation paper, page 42. See also note 24.

Loosening of consumer protections against direct marketing

Proposed Rule 7.5(3)(a)(iv) expands the permissible scope of direct marketing based on consumer data obtained through CDR. Whereas under the CDR Rules currently in force requesting consumer consent for direct marketing is allowable only for provision of a specific CDR good or service, the amendments expand parameters of consent for what constitutes acceptable direct marketing using imprecise and subjective language which will make it difficult for consumers or regulators to prove a breach of the Rule ("no more than a reasonable number" and "reasonably believes that the CDR consumer might benefit").
We do not support amendments to the CDR Rules that increase the capacity for direct marketing to consumers based on use of CDR data. According to results of our 2020 consumer survey, 73% of Australians are concerned by the extent to which their personal data is being used to target them for specific products or services[33].

We draw attention to the example of "companies using data about individuals to target them with sales approaches when they are at their most vulnerable" being described by ACCC Chair Rod Sims as an example of behaviour that "would be unlikely to be found to be unconscionable conduct, but is unfair and should be prohibited." [34] We consider this type of behaviour is facilitated by the combination of proposed Rules amendments in relation to use of CDR data for Research data and the loosening of direct marketing protection. We also agree with the view expressed in Update 2 to the PIA that lack of transparency about what arrangements are in place between Accredited Persons when consumers are being recommended certain goods or services increases the risk of vulnerable consumers being taken advantage of.[35] Expanding on this, we would contend this poses an unnecessary risk for every consumer.

Loosening of consumer protections against on-selling (deidentified) CDR data

Proposed Rule7.5(1)(aa)(iii) establishes a new permitted use for CDR data: "de-identifying collected CDR data for the purpose of disclosing (including by selling) the de-identified data; in accordance with a current use consent for that purpose from the CDR consumer". We query whether this is in effect allowing this purpose to *be* the use case. We also note the analysis given by Maddocks in Update 2 to the PIA: "The proposed amendments remove the restriction on asking a CDR Consumer for their consent to sell their CDR Data, and instead introduce a new restriction [which] means that an Accredited Person is not prohibited from asking a CDR Consumer for consent to sell their CDR Data when asking for any consent that falls into a category of consents."

We do not support any amendments to the CDR Rules that increase the capacity for CDR data to be on-sold by Accredited Persons, particularly when meaningful benefit of this proposal to consumers has not been articulated. According to results of our 2020 consumer survey, 90% of Australians

[33] CPRC Data and Technology Consumer Survey, conducted in partnership with Roy Morgan in March/April 2020.
[34] 'Tackling market power in the COVID-19 era'. Speech by ACCC Chair Rod Sims to the National Press Club, 21 October 2020. https://www.accc.gov.au/speech/tackling-market-power-in-the-covid-19-era
[35] Maddocks (2020), p50 (analysis of Risk 6).

object to companies on-selling their personal data.[36] We understand that government guidance relating to both CDR and the Privacy Act maintains that deidentified data is no longer considered to be personal data, however we suggest that consumer attitudes may not draw the same distinction. We highlight that statistical models can correctly reidentify 99.98% of individuals in any available anonymised dataset, using 15 common characteristics. Even with only four attributes (age, gender, date of birth, and marital status) 95% of individuals can be successfully reidentified.[37]

Other relevant Rules issues

Currently, the maximum historical range of CDR data will always be disclosed by Data Holders under a valid request (for example, up to seven years for banking transaction data). There is no provision for consumers to indicate consent for a limited range (ie, to consent to sharing data from the last 12 months and for the duration of consent, but nothing before that date). We believe this is an important element of consent which it would benefit consumers to have more influence over. More fundamentally, we are concerned that that the full extent of data to which CDR consents relate is not being made sufficiently clear to consumers.[38]

This issue is representative of our broader concerns that key elements of CDR will not be clearly understood by consumers, at the same time as more obligation for risk is being placed onto them under the scheme (and through parallel reforms, such as the proposed wind back of Responsible Lending Obligations). There is a significant risk of poor consumer outcomes if the substantial changes to the CDR Rules framework set out in the consultation paper are undertaken in a rushed manner and before effects of the initial scope of CDR have been seen and considered.

We welcome opportunities to provide ongoing input to the ACCC's CDR consultation process. For further discussions regarding our research or any of the positions expressed in this submission, please contact Nina Lewis, Research and Engagement Manager (CDR): nina.lewis@cprc.org.au

Lauren Solomon

Chief Executive Officer
Consumer Policy Research Centre

[36] CPRC Data and Technology Consumer Survey, conducted in partnership with Roy Morgan in March/April 2020. When asked to assess on a Likert scale how fair or unfair it is for a company to sell their personal information to other companies, 18% of survey respondents said the practice was "unfair", with a further 72% indicating they find it "very unfair".

[37] Rocher, L., Hendrickx, J.M. & de Montjoye, Y. (2019) 'Estimating the success of re-identifications in incomplete datasets using generative models'. *Nat Communications* **10,** 3069 (2019).

[38] We note there is a requirement in the existing Rules for data holders to inform consumers of the date range of CDR data that will be released (as part of authorisation of consent) and suggest this could be strengthened by also requiring data recipients to state as part of consent requests the maximum extent of data that will be covered by that consent. We also seek Rules that would allow the consumer to be able to specify consent to apply to a specific historical range of data, rather than having to consent to the full extent of historical data prescribed as CDR data under sector-specific Rules. This would help prevent unnecessary collection of CDR data and ensure better conformance to CDRs data minimisation principle.

Consumer Policy Research Centre

Level 14, 10-16 Queen Street, Melbourne, Victoria 3000

ABN 23 100 188 752 T 03 9639 7600 W cprc.org.au

Appendix 1 : List of prior CPRC submissions to public CDR consultations

- Submission by CPRC to Review into Open Banking

23rd March 2018

- Submission by Consumer Policy Research Centre to Treasury Laws Amendment (Consumer Data Right) Bill 2018- Exposure Draft

7 September 2018

- Submission by Consumer Policy Research Centre to Treasury Laws Amendment (Consumer Data right) Bill 2018: Provisions for further consultation and Designation Instrument for Open Banking

12 October 2018

- Submission by Consumer Policy Research Centre to ACCC- Consumer Data Right Rules Framework

12th October 2018

- Submission by Consumer Policy Research Centre to Senate Economics Legislation Committee Inquiry into Treasury Laws Amendment (Consumer Data Right) Bill 2019

28th February 2019

- Submission to the ACCC Consultation Paper: Data Access Models for Energy Data

22 March 2019

- Submission by Consumer Policy Research Centre to ACCC – Draft Rules Banking

10th May 2019

- CPRC Submission to The Treasury: Inquiry into Future Directions for the Consumer Data Right: Issues Paper

25th May 2020

- Submission to Consumer Data Right Energy Rules Framework Consultation Paper

28th August 2020

- Submission to Treasury Consultation on Consumer Data Right Legislative Amendments

21 October 2020