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

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

12th October 2018

Email: ACCC-CDR@accc.gov.au

Dear Secretariat,

The Consumer Policy Research Centre (CPRC) would like to thank you for the opportunity to respond to the Consumer Data Right (CDR) Rules Framework.

CPRC is an independent, not-for-profit consumer research organisation. CPRC undertakes interdisciplinary and cross-sectoral research to inform policy reform and practice change. Our goal is to achieve a fair outcome for all consumers. Consumer data is a central research priority for the organisation due to the rapidly growing online marketplace, early adoption of digital technology by Australians, and the emerging benefits and risks to consumers of Big Data amalgamation.

We would like to raise with the consultation team the significant number of policy processes underway in relation to the management, sharing and release of data impacting consumers. The ability of policymakers to fully consider the benefits and risks of such reforms relies upon the ability for consumer organisations to participate in such processes. CPRC strongly encourages the Australian Government to - in light of the rapid transformation required in the digital economy - make provisions to adequately fund consumer representatives to participate in these processes.

CPRC would like to acknowledge the efforts by policymakers and regulators to improve the consent, privacy and consumer experience of data proposed to be shared via the CDR system. We acknowledge the considerable focus and thought that has been put in the CDR Rules Framework regarding the minimum conditions for consent and the recommendation of a consent user testing process. We encourage the ACCC to further consult with experts regarding adequate protections for minors and other vulnerable groups such as consumers experiencing domestic violence.

We also continue to highlight the benefit and need for the implementation of economy-wide reforms in Australia alongside the introduction of the CDR. Such changes are needed to manage and minimise the potential harm of data leakage outside of the CDR where there is lower or in some instances no protection for consumer privacy and CDR data. For the CDR regime to garner consumer trust and uptake, consumers need to be provided with the confidence that their data will be adequately protected.

In addition to this, where possible, the Rules Framework should strive to achieve Privacy by Design and facilitate processes to improve consumer understanding and control over their data. This includes concepts such as data deletion by default where the data has become redundant or accreditation has been revoked, and a centralised dashboard for consumers to manage their data and consent.

## Recommendation 1: Manage and minimise data leakage outside of CDR

CPRC does not support the current position in the CDR Rules Framework that *"In relation to transfer of data outside of the CDR regime and transfer of data overseas, the ACCC recognises the potential risks with these uses but given the stringent rules the ACCC proposes in relation to consent under the CDR regime generally (where all uses are required to be disclosed), the ACCC considers that additional requirements will not be needed in the rules"* (pg39)[1].

CPRC believes the risk of data transfers out outside of the CDR regime is still significant as outlined further below.

***The need for economy-wide data protection***

In our submission to the Treasury Laws Amendment (Consumer Data Right) Bill 2018 in September 2018[2], we highlighted the problems regarding the complexity of having dual privacy frameworks operating under the Consumer Data Right, and in some instances three operating where the European Union's (EU) General Data Protection Regulation (GDPR) may also apply. The dual privacy frameworks that may be 'switched on' or 'off' depending on the type of CDR participant and consumer data involved introduces complexity for businesses in understanding their compliance obligations, as well as for consumer in understanding their legal rights and presumably also for regulators and policymakers developing an adequate compliance and monitoring regime.

Furthermore, the current drafting of the Rules Framework suggests CDR data can be provided to non-accredited third parties. Page 49 states that *"The ACCC recognises that there will be instances where a consumer wishes to have their CDR data disclosed to a non-accredited entity. For example, a consumer might want to have their data disclosed to their accountant to assist in the preparation of their tax return"*[3].

While we recognise that there may be classes of entities that have legitimate cases to access the data, the ability to disclose CDR data to non-accredited third parties is problematic because non-accredited third parties are not governed by the privacy safeguards offered by the CDR, and some may not even be captured under the Privacy Act, for example, small businesses with a turnover of less than $3 million. Therefore, in some instances, consumers have no privacy protection at all when it comes to CDR data being ported outside the system being developed.

---

[1] ACCC. Consumer Data Right Rules Framework. Available at https://www.accc.gov.au/focus-areas/consumer-data-right/accc-consultation-on-rules-framework (Accessed 8 Oct 2018)

[2] Consumer Policy Research Centre. Submission by Consumer Policy Research Centre to Treasury Laws Amendment (Consumer Data Right) Bill 2018- Exposure Draft. Available at https://static.treasury.gov.au/uploads/sites/1/2018/09/t329531-Consumer-Policy-Research-Centre.pdf

[3] Ibid. ACCC. Consumer Data Right Rules Framework.

This is particularly concerning if there are predatory firms that do not need to comply with either framework. Without a whole of government approach to reform economy-wide data protection, we risk losing consumer trust and effective participation in the CDR framework. This is particularly important as the CDR aims to eventually extend to datasets and data sharing across the economy, not just in banking. We reiterate our strong recommendation to policymakers and regulators to strive for economy-wide protections and reform to ensure that we are opening up consumer data in a safer environment.

***Lower tiers of accreditation for certain classes of providers***

In the absence of economy-wide reform, we then strongly recommend that the ACCC develop a framework with higher protections for data that may be ported by the consumer outside the CDR system. CPRC recommends that the ACCC either consider a tiered accreditation system or exemption process for certain classes of use where there is clear evidence of benefit, such as accountants and financial counsellors, where the use case and volume of need to access data via CDR is clear, rather than allowing data to be transferred to non-accredited third parties for any circumstance where the privacy safeguards no longer apply.

Consultations with accountants, financial counsellors and other proposed classes of data recipients about their potential uses of CDR data, what types of CDR data would be required, and internal resources available to them, may help to inform the criteria for lower tiers of accreditation or exclusion categories. Having these classes of users included as accredited data recipients could also mean that the CDR consumer can continue to use secure channels to port their data and allow regulators to monitor and better understand how CDR data is being used in the regime.

As we outline in our earlier submission to the Treasury Laws Amendment (CDR) Bill 2018 (stage 1)[4], allowing data to be disclosed to non-accredited entities essentially creates a 'back-door' mechanism to accessing more data about consumers without the need to be an accredited entity. This may expose the data in an environment where there are weaker privacy safeguards and lower consumer control over their data. For example, a non-accredited entity might only give a consumer access to services on the condition that they provide more sensitive CDR data than is necessarily required. The consumer might have little to no control over the provision of this data, particularly if it could impact their fundamental rights in future to accessing products or services such as housing, telecommunications or utilities. This is likely to undermine consumer trust in the CDR framework which has been pitched to provide consumers with more control and protection of their CDR data. It also acts as a disincentive for entities to participate in the CDR framework because they can access the data through alternative pathways without being subject to CDR regulations.

Therefore, in the absence of economy-wide data protection reform, allowing disclosures of CDR data to non-accredited entities is not recommended. Rather classes of potential data recipients should be reviewed (or apply to be reviewed) to decide whether they should be included in a lower tier of accreditation, or if accreditation is unreasonable, be provided an exemption

[4] Ibid. Consumer Policy Research Centre. Submission by Consumer Policy Research Centre to Treasury Laws Amendment (Consumer Data Right) Bill 2018- Exposure Draft.

framework to use the CDR data only for a specific purpose with appropriate privacy protections put in place as approved by the ACCC and OAIC.

CPRC is supportive of a register of accredited CDR participants to promote transparency and accountability. We agree that there should be Rules to specify the way accredited participants are permitted to describe their accredited status.

## Recommendation 2: Privacy by Design- deletion by default

***When data becomes 'redundant'***

The current draft of the revised Bill (pg21- Privacy safeguard 12)[5] and Rules framework (pg56- Safeguard 11)[6] suggests that if the accredited data recipient no longer needs the CDR data for the purposes permitted under the CDR Rules and is not required to retain the data by law, the data is 'redundant' and they can either destroy or retain the CDR data as de-identified data. The data is also considered 'redundant' if a consumer withdraws consent (pg38 of CDR Rules Framework).

The ACCC suggested that *"While the Open Banking review did not recommend a right of deletion, allowing accredited data recipients the ability to retain consumers' data at their discretion, albeit de-identified, may not be consistent with the consumer-centric aims of Open Banking".* CPRC notes that the ACCC is seeking views regarding the extent to which a consumer should be able to decide whether their redundant data is de-identified or destroyed.

Ultimately, the decision as to whether the information should be deleted or de-identified should not be left to the accredited data recipient to decide. While we agree that consumers should have a choice as to whether they agree to have their information de-identified, a Privacy by Design[7] approach is recommended to delete the data by default once use permission has been spent. This still preserves consumer choice to elect to have their data kept de-identified if they would like to contribute their data after use permission has been spent. If consumers have withdrawn consent, the data should certainly be destroyed by default if data retention is not required by law.

We generally agree with ACCC's proposal regarding how consent must not *"rely on default settings, pre-selected options, inactivity or silence" (pg32)*— as a strategy to appropriately counter 'dark patterns'[8]. Dark patterns are interface design strategies used in websites or apps

[5] The Treasury. Treasury Laws Amendment (Consumer Data Right) Bill 2018 (second stage) and Designation Instrument for Open Banking. Available at https://treasury.gov.au/consultation/c2018-t329327/ (Accessed 5 Oct 2018)

[6] Ibid. ACCC. Consumer Data Right Rules Framework.

[7] Information and Privacy Commissioner of Ontario (IPC). (2013). Privacy by design. Information and Privacy Commissioner of Ontario. Available at https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf (Accessed 11 Oct 2018).

[8] Dark Patterns. (n.d.). What are Dark Patterns? Dark Patterns. Available at https://darkpatterns.org/ (Accessed 8 Oct 2018)

to steer consumers to behave in ways that may not be in their best interest[9,10]. Regarding the proposal to delete the data by default, this preserves privacy *in the interest* of the consumer and we would be supportive of informing consumers of this default setting.

Allowing the data recipient to store the CDR data as de-identified data serves a secondary purpose and would generally be separate to the consumer's primary consent to a specific use case because this de-identification occurs when the data becomes 'redundant'. We suggest a cautious approach by proposing deletion by default because the alternative of de-identifying unit record level information still presents significant risk of re-identification[11,12], which may not necessarily be well understood by the consumer. This is particularly important when we do not know what the data may be used for. Furthermore, the risk may increase over time as more data sharing and amalgamation is enabled across sectors by the CDR, where de-identifiable information could be overlaid to re-identify and accurately target consumers in ways that may not be in the interest of the consumer. This can arguably be facilitated legally because the data is deemed as 'de-identified' and therefore not personal information under the Privacy Act.

The level of risk may not necessarily be fully comprehended by consumers and therefore deletion by default is recommended for sensitive data such as banking data.

In relation to the setting of defaults, CPRC refers the ACCC to Professor Cass Sunstein's, co-author of Nudge recently proposed Bill of Rights for Nudging which entails five key principles when considering the ethics of using nudges in a range of settings:[13]:

1. Nudges must be consistent with people's values and interests;
2. Nudges must be for legitimate ends;
3. Nudges must not violate anyone's individual rights;
4. Nudges must be transparent; and
5. Nudges ought not to take things from people without their consent

The setting of defaults is a well-known nudge and taking into consideration the fifth principle that a nudge should not take things away from people without their consent. Given the significant evidence that de-identified data can easily be re-identified through sophisticated (and sometimes unsophisticated) data matching techniques, and the clear risk for this data in future to potentially be used to disadvantage consumers, we would strongly recommend careful consideration by the ACCC of the setting of defaults which enable such a risk.

---

[9] Ibid. Dark Patterns. (n.d.). What are Dark Patterns? Dark Patterns.
[10] Forbrukerradet. (2018). Deceived by Design. Forbrukerradet. Retrieved from https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/
[11] Teague, V., Culnane, C., Rubinstein, B. (2017). The simple process of re-identifying patients in public health records. Pursuit. The University of Melbourne. Available at https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records (Accessed 8 Oct 2018)
[12] De Montjoye, Y., Radelli, L., Sing, V.K., Pentland, A.S. Unique in the shopping mall: On the reidentifiability of credit card metadata. Science 2015;347(6221): 536-539
[13] Easton, S. Cass Sunstein's Bill of Rights for Nudging. The Mandarin. Published 19 Jul 2018. Available at https://www.themandarin.com.au/96009-cass-sunsteins-bill-of-rights-for-nudging/ (Accessed 8 Oct 2018)

CPRC can anticipate some situations where a consumer might want to opt in to allow their data to be retained de-identified. For example, if some entities proposed to use de-identified data as a tool to assist regulators in detecting and monitoring discriminatory practices affecting vulnerable groups, consumers might feel that this is a valid and useful purpose for contributing their data. Consumers would be notified of the request and provided with the option to consent for this purpose.

We recommend the ACCC develop or adopt Rules for de-identification standards which may be developed or advised by the Data Standards Body or other designated technical expert as a minimum requirement for de-identification of CDR data. Additionally, the data should not be released as public data or shared with other entities in unit record level.

Lastly, in order for consumers to trust the CDR regime, the extent to which consumers have control over their data through consent must be fully considered. CPRC proposes that the data should be deleted if consent is withdrawn to uphold consumer's consent. Furthermore, this places pressure on companies to act responsibly and respect consumer values or otherwise risk losing their data.

***When accreditation is revoked***

Where a decision has been made to revoke the data recipient's accreditation, CPRC strongly recommends that the Rules require the data recipient to delete the CDR data, rather than giving them the option to either delete or de-identify the CDR data. CPRC supports the conditions provided in section 6.7 to determine revocation of accreditation. Given the serious nature of the reasons to revoke accreditation, CPRC believes that it would be in the best interest of consumers if the data is deleted rather than retained as de-identified data by the data recipient. Furthermore, CPCR suggests that both the suspended and revoked accredited data recipients' obligations in relation to CDR data should continue to apply.

***Rules to prohibit on-selling of CDR data for direct marketing***

*"In relation to on-selling of data and use of CDR data for direct marketing, the ACCC's current position is that it proposes to make rules that will prohibit the use of CDR data for these purposes"* (pg39).

CPRC supports this position and recommends that this should be extended to 'redundant data'. Should the consumer wish to have their data used for direct marketing, it must be based on informed and free consent, and consumers must be able to withdraw their consent and have their data deleted under the CDR regime.

## Recommendation 3: Protection of minors and other vulnerable groups

CPRC does not agree with the position in the CDR Rules Framework that minors should be treated the same as any other consumer who may take advantage of the CDR. Further consideration and consultation with experts who work with children are recommended.

Article 8 of the GDPR suggest that *"in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only*

*if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years"*[14]. The Australian Institute of Family Studies has identified the need for parents to be involved with children and young people's online safety, suggesting that "*children and young people are at a dynamic stage of development in which risk-taking behaviours and emerging decision-making can lead to negative outcomes*"[15]. There is merit in exploring whether the limitations on the processing of children's data proposed in the GDPR should also be similarly applied to the CDR regime or further protections should be considered given the sensitive nature of sharing banking data, the inferences that can be made from the data, and how the data may impact their current and future access to products and services.

Some potential benefits of the CDR identified by Treasury included (but not limited to)[16]:

- Comparison tools to provide product recommendations (credit cards, mortgages, business lending products) tailored to actual spending and repayment patterns
- Budgeting tools to assist consumers in better managing their finances
- Services to provide businesses with insights or assist them in meeting compliance obligations.

However, CPRC feels that the risks outweigh the benefits for minors as they have lower capital and higher risk of data exploitation compared to other CDR consumers. Data that is retained about minors may present risk of creating a digital profile based on their habits and purchasing behaviour during a stage of their life where they are still developing and should be afforded greater protections and privacy. These profiles may potentially result in unfair outcomes for these individuals in accessing products and services in the future, if there are inadequate protections in place.

CPRC appreciates that there are circumstances where a young person might move out of home and become an independent, thereby requiring more autonomy over their financial data. It is not our intention to restrict these minors from making independent decisions regarding consent for sharing their CDR data. CPRC encourages the ACCC to consult with organisations who have expertise in working with vulnerable groups including minors and people experiencing domestic violence to ensure that any harms that may arise through the standard CDR consent process can be adapted to minimise negative outcomes.

[14] Intersoft consulting. (n.d). Article 8 GDPR. Conditions applicable to child's consent in relation to information society services. Available at https://gdpr-info.eu/art-8-gdpr/ (Accessed 5 Oct 2018)
[15] Australian Institute of Family Studies. Online Safety. Published April 2018. Available at https://aifs.gov.au/cfca/publications/online-safety (Accessed 5 Oct 2018)
[16] The Treasury. Consumer Data Right 9 May 2018. Available at https://static.treasury.gov.au/uploads/sites/1/2018/05/t286983_consumer-data-right-booklet.pdf (Accessed 8 Oct 2018)

## Recommendation 4: Centralised dashboard for consumers rather than multiple dashboards

On pg38 of the Rules Framework *"The ACCC proposes to make rules that will require all accredited data recipients to have a system in place which allows consumers to readily manage their consents. This should allow consumers to view what they have consented to and to readily withdraw those consents if they choose".*

While CPRC is supportive of the idea of a dashboard, we are concerned that having multiple dashboards with different providers may become confusing and difficult to manage for consumers when they begin to port their data to multiple entities. This may become increasingly difficult in the future where CDR data can be ported across different sectors. CPRC proposes that a centralised dashboard be created by the Data Standards Body or other appropriate technical expert, where consumers are able to manage their CDR data and consent holistically. Further consultation with technical experts is required to explore the security requirements and risks that should be considered. At a minimum, the centralized portal should be a useful visual tool for consumers to monitor the history of their CDR consent and usage.

A centralised 'portal' for privacy management is not a new concept. This has been proposed by privacy experts such as Professor Daniel Solove[17] to improve practicability in managing privacy, and by the Federal Trade Commission in relation to improving data transparency and accountability of data brokers[18]. CPRC proposes the ACCC set Rules for data holders and data recipients to participate in a centralised dashboard and consult with the Data Standards Body to operationalise the dashboard.

Another challenge is how to provide consumers with awareness and understanding of when the privacy safeguards are 'switched on' or 'off' for their CDR data, which perhaps could also be incorporated into the dashboard. The latest draft of the Treasury Laws Amendment (Consumer Data Right) Bill 2018 (provisions for further consultation)[19] suggests there is a very complex logic for understanding legal protections, for example it suggests that most privacy safeguards do not apply to accredited data holders and that historical CDR provided to accredited data recipients may be subject to the Australian Privacy Principles (APPs) instead of the privacy safeguards if the data recipient becomes the data holder—made possible under the Rules in example 1.7 of the explanatory materials:

> *"Max is a consumer with AllenBank. All of his transaction information held by AllenBank is treated consistently with the Privacy Act and APPs by AllenBank.*
>
> *Max has a transaction (savings) account with AllenBank but has been told by friends he can probably get a better interest rate elsewhere. Keen to make the most of the CDR, Max has requested AllenBank to transfer his CDR data relating to the transaction account to HIZAI Banking Services.*

---

[17] Solove, DJ. Introduction: Privacy self-management and the consent dilemma. Harvard Law Review. 2013, 126 (7): 1880-1903

[18] Federal Trade Commission. (2014). Data Brokers. A Call for Transparency and Accountability. Federal Trade Commission. Retrieved from https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[19] Ibid. The Treasury. Treasury Laws Amendment (Consumer Data Right) Bill 2018 (second stage) and Designation Instrument for Open Banking.

*At the time of receiving Max's CDR data, HIZAI Banking Services is required to handle the data in accordance with the CDR Privacy Safeguards because HIZAI Banking Services is an accredited data recipient in respect of Max's data.*

*Max discovers that HIZAI Banking Services will provide him with a better interest rate on his transaction account. Max closes his transaction account with AllenBank and opens an account with HIZAI Banking Services.*

*All new transaction data created by HIZAI Banking Services in relation to Max's transaction account is subject to the Privacy Act and the APPs.*

*Consumer data rules may enable HIZAI Banking Services to also treat Max's historical data as a data holder, and subject instead to the APPs."*

This again points back to the need for a consistent, economy-wide data protection reform as the current system is overly complex and may still be difficult to comprehend even with a centralised dashboard.

At a minimum, it is CPRC's view that historical CDR data should continue to be subject to privacy safeguards even if the accredited data recipient becomes the data holder for that information.

CPRC supports the rule that accredited data recipients will remain responsible and liable for compliance with all obligations under legislation, Rules and standards, for any outsourcing arrangements with a service provider involving the disclosures of CDR data. It is important for CDR consumers to understand that their data is still protected in these settings to facilitate participation. However, there is a risk of confusion regarding legal protection for outsourcing arrangement compared to sharing with non-accredited third-party recipients given the complexity in explaining the varying data protection arrangements.

Providing consumers and CDR participants with the education to accurately decipher the varying settings for when APPs, privacy safeguards or no data protection applies will remain a big challenge.

## Recommendation 5: Provision of datasets including consumer's product information based on their applicable rates and profiling information to consumers

CPRC supports ACCC's proposal *"to make rules to the effect that the product data specified in section 5.3.3, as it relates to an account or accounts that a customer holds, is within scope. This will ensure that the features of the account that the individual customer holds, such as applicable fees, charges or interest rates on that account, can be shared"* (pg19).

It is important that consumers are given access to their product information and features, for example the rates they are actually being charged, and not limited to product feature information that they were advertised when they initially joined. Product information including applicable rates and features/benefits are needed for accurate product comparisons so that consumers can make informed decisions around switching.

CPRC also recommends ACCC to consider making recommendations about giving consumers access to their profile information/category/score (i.e. transformed or value-added data) to

reduce data asymmetry, and to provide them with explanation as to why they may or may not be eligible for certain products or services. Any further sharing of this information should only be at the direction of the consumer, following informed consent that is freely given.

## Recommendation 6: Reciprocity of data sharing should only be allowed at the direction and consent of the CDR consumer

*"The ACCC does not understand the principle of reciprocity to mean that a data holder is entitled to request or obtain data from an accredited data recipient before sharing data it has been directed to share by a CDR consumer. Reciprocity is not a 'quid pro quo' arrangement between data holders and accredited data recipients. The CDR regime is consumer focused, and any approach to reciprocity would need to be based on a consumer directing and consenting to an accredited data recipient sharing their data"* (pg21).

CPRC is supportive of ACCC's position that any approach to reciprocity would need to be consumer focused and at the direction of the consumer, provided consent is freely given.

## Recommendation 7: Allowing use of pseudonyms or anonymity for comparative purposes

The Explanatory Materials[20] (provisions for further consultations) and the ACCC Rules Framework[21] suggest that that consumers will be prohibited from using a pseudonym for this sector.

CPRC suggests that Treasury and ACCC reconsider prohibiting the use of pseudonyms or anonymity for Open Banking because this should be offered to consumers who wish to access tools to compare and receive product recommendations. The consumer should not be under any obligation to share their identity if they are not signing up to receive the product or service. For example, a consumer comparing flights, health insurance, energy would not need to disclose their identity in order to receive product recommendations. It is generally at the point of sale that they provide their details.

## Recommendation 8: Develop user centric interfaces and consumer testing for comprehension

CPRC supports ACCC's proposal *"to make rules that the authorization standards are subject to consumer testing, consideration by the Data Standards Body's user experience consultative group, and meet certain service level requirements/non-functional requirements"* (pg42).

User testing is important to ensure that the information is easily understood and that there are no unintended 'dark patterns' that are embedded in the design. Testing with a diverse group of

[20] The Treasury. Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation. Explanatory Materials. Available at https://static.treasury.gov.au/uploads/sites/1/2018/09/Explanatory-Materials-Provisions-for-further-consultation-1.pdf (Accessed 11 Oct 2018)

[21] Ibid. ACCC. Consumer Data Right Rules Framework.

end users will be important to check for elements for inclusive design. Particular groups who may want to access the CDR but may experience barriers or higher vulnerability should also be considered such as the elderly, people with disability, and people from culturally and linguistically diverse backgrounds. It is also important to consider the risks to these populations in accessing the CDR regime to include added protections as appropriate. There may be a number of reasons why some members of these groups might bank offline, such as having an inability or lack of confidence in accessing online technology. We appreciate that there may be challenges to including offline consumers by 1 July 2019 due to the way requests, authorisation and authentication are currently proposed. However, we want to ensure that these groups do not get left behind in accessing benefits and therefore should not be forgotten in later stages. Mechanisms for offline consumers to access and port their data should be considered as the CDR evolves.

CPRC and QUT have recently partnered on a project with Thoughtworks and the Office of the Information Commissioner Queensland *Putting End-Users in Charge of Algorithms* to co-design notification and consent prototypes that will showcase privacy and autonomy by design. The project will engage with end users and interdisciplinary experts such as software engineers, interactive designers, policy makers and government representatives. We welcome further support from and engagement with policymakers and regulators on this project as we believe it could provide significant insights to inform the CDR consent regime development. The pilot project may also have broader application should an economy-wide reform be introduced.

If you have any questions or would like further information regarding this submission, please don't hesitate to contact the CPRC office@cprc.org.au.

Yours sincerely,

Lauren Solomon

Chief Executive Officer

**Consumer Policy Research Centre**

## About Consumer Policy Research Centre (CPRC)

An independent, non-profit, consumer think-tank established by the Victorian Government in 2016, CPRC undertakes consumer research independently and in partnership with others to inform evidence-based policy and business practice change. Our vision is to deliver a fair outcome for all consumers. We work closely with policymakers, regulators, academia, industry & the community sector to develop, translate and promote evidence-based research to inform practice and policy change.