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 Treasury Laws Amendment (Consumer Data right) Bill 2018: Provisions for further consultation and Designation Instrument for Open Banking

12 October 2018

Email: data@treasury.gov.au

Dear Mr. McAuliffe,

The Consumer Policy Research Centre (CPRC) would like to thank you for the opportunity to respond to the Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation and Designation Instrument for Open Banking.

Treasury provides the following explanation for why a Consumer Data Right regime is an important initiative: *"the primary aim of the Consumer Data Right (CDR) is to give consumers the ability to access more information about themselves, and about their use of goods and services, in a manner that allows them to make informed decisions about both themselves and their participation in the market"*[1].

In line with these aims and our initial submission to the Treasury Laws Amendment (Consumer Data Right) Bill 2018 exposure draft, CPRC continues to hold the view that:

- The Consumer Data Right should be renamed to the Data Portability/Transfer Right to more accurately reflect its functions;
- There is a significant need for a whole-of-government approach to economy-wide data protection reform to address the risk of CDR data leakage outside the system;
- CDR data should be prevented from transfers to non-accredited third parties in the absence of reform to economy-wide data protection. Entities such as accountants and financial counsellors with legitimate cases for using CDR data should be considered for lower tier accreditation or exemptions, thereby ensuring they are still covered under the CDR Privacy Safeguards;
- Privacy by Design be embedded in the legislation by ensuring redundant data is deleted by default;
- Consumers should be provided with their CDR information for free without restrictions. If a cost must be considered for some high-level derived data, consumers should still be provided at least a free copy once a year, a similar model to requesting a credit report

[1] The Treasury. Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation. Proposals. Available at https://static.treasury.gov.au/uploads/sites/1/2018/09/CDR-proposals-for-further-consultation-1.pdf (Accessed 10 Oct 2018)

- Consumers should also have access to profiling information/categories/scores observed or *generated* relating to them (i.e. transformed or value-added data), and not limited to just accessing information that were observed or provided *by* the person;
- Legislating CDR participants to participate in a centralised dashboard would greatly assist consumers in managing their consent and data portability over time and especially as new sectors are brought into the CDR system.

Further to this, we would like to respond to proposed changes to the Bill and the Designation Instrument for Open Banking.

Recommendation 1: Requiring consistent application of Privacy Safeguards for all CDR participants including data holders and data recipients

Page 6 of the proposal paper[2] also states that *"a range of submissions suggested that it was unclear from the exposure draft of the Bill whether and when they would need to comply with the Privacy Safeguards, the Privacy Act or both. To clarify the interactions between the laws, Treasury proposes that most of the Privacy Safeguards will not apply to data holders. Further, only the Privacy Safeguards (and not the Privacy Act) will apply to data recipients, in respect of the CDR data they have received"*.

Aside from ongoing concerns that we have raised about unnecessary privacy complexity for all parties being introduced as a result of this reform, it is CPRC's view that all CDR participants (both data holders and data recipients) should be subject to the Privacy Safeguards for CDR data. The proposal to change some of the Privacy Safeguards from applying to CDR participants (i.e. both data holders and data recipients) in the first version to now fewer Privacy Safeguards applying to data holders does not add clarity—rather it adds even *more* complexity to understanding obligations and protections in the CDR regime.

It is also unclear why the proposal is suggesting that accredited persons have fewer applications of the Privacy Safeguards compared to accredited data recipients (see table on pg2 of the proposal paper)—the application should be the same as that for accredited data recipients. It is not clear in the meaning provided of accredited data recipients on pg7 of the inserts in the exposure draft[3], how an accredited person is different to an accredited data recipient.

CPRC recommends a consistent approach within the CDR framework regarding Privacy Safeguard applications.

We remain concerned that the sharing of sensitive data facilitated via the CDR regime outside the Privacy Safeguards will in some cases, leave consumers with no privacy protection. For instance, when the data is leaked out of the CDR system and the entity collecting the data is a

---

[2] Ibid. The Treasury. Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation. Proposals.

[3] The Treasury. Inserts for Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation. Available at https://static.treasury.gov.au/uploads/sites/1/2018/09/Treasury-Laws-Amendment-Consumer-Data-Right-Bill-2018-Provisions-for-further-consultation-1.pdf (Accessed 10 Oct 2018)

small business with a turnover of less than $3 million -under this circumstance consumers are neither protected by the Privacy Safeguards or the Australian Privacy Principles (APPs).

We continue to recommend economy-wide data protection reform to address the risk of data leakage outside the CDR framework where other privacy frameworks with lower protections operate. 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.

Recommendation 2: Introducing classes of entities under lower tier accreditation where the benefit, use case and volume of need to access data via CDR is clear—rather than permitting data transfers to non-accredited entities

CPRC recognises that there may be legitimate cases to transfer CDR data to particular entities other than Authorised Deposit-Taking Institutions (ADIs), such as accountants or financial counsellors. We agree that consumers should not be prevented from using their CDR data that may be needed to access these services for specific purposes, such as preparing their tax return. CPRC proposes that potential classes of data recipients could be reviewed (or apply to be reviewed) for the ACCC to determine whether they should be included in a lower tier of accreditation, or if accreditation is unreasonable, be provided an exemption 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.

As we raised in our earlier submission to the stage one consultation of the Bill[4], allowing data to be disclosed to non-accredited entities 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. In the absence of economy-wide data protection reform, general disclosures of CDR data to non-accredited entities should not be permitted.

Recommendation 3: Embedding Privacy by Design in legislation requiring deletion by default

Deletion by default for redundant data

It is CPRC's view that the provisions for *"56EN Privacy safeguard 12—security of CDR data held by accredited data recipients"* is insufficient[5].

Section 2 suggests that if the person (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

---

[4] 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

[5] Ibid. The Treasury. Inserts for Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation.

data is 'redundant', and they can either destroy or retain the CDR data as de-identified data. This is contrary to providing consumers with control over their CDR data.

CPRC recommends that the decision to whether the information should be deleted or de-identified should not be left to the accredited data recipient to decide, and that the data should be deleted by default. Deletion by default should be embedded into the legislation based on Privacy by Design principles[6].

There are several reasons for this:

- de-identifying unit record level information still presents significant risk of re-identification[7,8]
- deletion by default enforces Privacy by Design, to counter dark patterns that can be embedded in websites or applications to steer consumers to behave in ways that may not be in their best interest[9,10]
- 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 can still preserve the 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.

Even with the option to opt-in however, CPRC believes there is still considerable risk that may not be fully comprehended by consumers.

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.

---

[6] 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).

[7] 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)

[8] 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

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

[10] Forbrukerradet. (2018). Deceived by Design. Forbrukerradet. Retrieved from https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

In relation to the setting of defaults, CPRC refers the Treasury 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[11]:

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 Treasury of the setting of defaults which enable such a risk.

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 that any de-identification must follow minimum standards developed or advised by the Data Standards Body or other designated technical expert, unless the accredited data recipient is able to demonstrate more robust techniques for de-identification. Additionally, the data should not be released as public data or shared with other entities in unit record level.

Deletion when consent is withdrawn or when accreditation has been revoked

CPRC proposes that Privacy Safeguard 12 includes requirements for deletion when consent is withdrawn and when accreditation is revoked.

Consumers may choose to participate under the CDR with the misbelief that they have full control of their data, which is untrue if they do not have the ability to have their data deleted when consent is withdrawn. Deletion of data under these circumstances is critical to gain consumer trust in the CDR regime. Furthermore, this places pressure on companies to act responsibly and respect consumer values or otherwise risk losing their data.

Lastly, given the serious nature of the reasons to revoke accreditation, CPRC believes it would be in the best interest of consumers for the data to be deleted if accreditation has been revoked.

[11] 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)

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

Recommendation 4: Data sets about consumers is fee free in the designation instrument

We note that *"Treasury proposes that the designation instrument for data sets should identify whether a data set is fee free or the data holder can impose charges for access and use (a chargeable dataset). Where fees may be imposed, market based pricing would be the initial price approach. The ACCC would have powers to determine a reasonable price for access if data holders impose excessive fees (taking account a range of factors, similar to current access regimes) … As recommended by the Open Banking Review, the data sets in the banking designation instrument would not be chargeable data sets"* (pg9 of proposal paper)[12].

CPRC supports the recommendation by Open Banking Review that the data sets in the banking designation instrument should be free.

In line with the CDR aim "*to give consumers the ability to access more information about themselves, and about their use of goods and services, in a manner that allows them to make informed decisions about both themselves and their participation in the market"*, we propose that consumer profiling information/category/scores should also be included.

We recommend changes to the designation instrument to state that consumers can also have access to information observed or *generated* relating to them (i.e. transformed or value-added data), in addition to accessing information that were observed or provided *by* the person, as described on p2 of the designation instrument (section "*Specified classes of information—information about user of product"*)[13].

CPRC recommends providing consumers access and explanation to information on consumer profiles or segments derived from their CDR data or other means, which can have an impact on the products or services they can access. This information may help to reduce data asymmetry between 'buyers' and 'sellers' so that consumers can make informed decisions about themselves and their participation in the market.

CPRC believes this information should also be provided to consumers for free, as any fees would act as a barrier for consumers to access this information. If a fee must be implemented for some high-level derived data, CPRC recommends at a minimum, that this high-level derived data be provided to consumers for free at least once a year, a similar model to requesting a credit report[14]. CPRC is also supportive of the ACCC in having powers to determine a reasonable price if data holders impose excessive fees.

---

[12] Ibid. The Treasury. Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation. Proposals.

[13] The Treasury. Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2018. Exposure Draft. Available at https://static.treasury.gov.au/uploads/sites/1/2018/09/Open-Banking-Designation-Instrument-1.pdf (Accessed 11 Oct 2018)

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

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

The description about *"Specified classes of information—information about a product"* on pg2 of the designation Instrument[14] outlines:

"(1) This section applies to information about a product, including, but not limited to, the following:

(a) a fee or charge associated with the product;
(b) an interest rate associated with the product;
(c) a feature or benefit of the product;
(d) the terms and conditions on which the product is offered or supplied;
(e) the eligibility criteria a person must meet in order to be supplied the product.

(2) Without limiting subsection (1), the information may relate to the product as offered or provided to particular classes of customers, or as tailored to a particular customer"

CPRC agrees that consumers should be provided the product information listed in section 1. It is essential that consumers are given access to their product information, for example the rates they are actually being charged, and not limited to product information that they were advertised when they initially joined. Applicable product information is needed for accurate product comparisons so that consumers can make informed decisions around switching.

CPRC recommend that it is made more explicit in the instrument that the product information is not limited to product information that was initially advertised, and includes product information that is currently being applied to the consumer.

Recommendation 6: Not place a limit to when ACCC can place emergency rules to avoid serious risk of harm to consumers

Page 8 of the proposal paper[15] states that *"Treasury proposes… to limit the circumstances in which emergency rules may be made to when the ACCC is of the opinion that an emergency rule is necessary to avoid imminent risk of serious harm to the efficiency, integrity and stability of the Australian economy, or to consumers."*

CPRC does not understand why such a proposal was put forward. As we discussed earlier, CPRC has serious concerns about data leakage outside of the CDR system and other risks that may affect vulnerable groups disproportionally. Given the CDR regime involves highly sensitive data, and is within its infancy, there needs to be no restrictions regarding emergency rules to address any unforeseen risk that emerges. CPRC is supportive of the ACCC in having powers to decide when to place emergency rules to avoid risk of serious harm to consumers. The Rules

[14] Ibid. The Treasury. Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2018. Exposure Draft.
[15] Ibid. The Treasury. Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation. Proposals.

can then be further consulted and reviewed as to whether they are made permanent or are amended.

Recommendation 7: Put in place protection for minors and other vulnerable groups

Minors have a greater risk of harm from participating in the CDR regime. 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*"[16].

There have been examples of protections put in place for minor's data internationally. 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"*[17].

Some potential benefits of the CDR identified by Treasury included (but not limited to)[18]:

- 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 currently outweigh the benefits without added protections, especially 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 recommends that Treasury put in place protections for minors and other vulnerable groups in the legislation. It is not our intention to restrict minors from accessing the CDR if there is a clear benefit, for example, under some circumstances for independent minors who have moved out of home.

---

[16] Australian Institute of Family Studies. Online Safety. Published April 2018. Available at https://aifs.gov.au/cfca/publications/online-safety (Accessed 5 Oct 2018)

[17] 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)

[18] 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)

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

Other vulnerable groups that could be considered are people experiencing domestic violence, the elderly, and people with low literacy.

Recommendation 8: Allowing use of pseudonyms or anonymity for comparative purposes

The Explanatory Materials[19] (provisions for further consultations) and the ACCC CDR Rules Framework[20] 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 necessarily need to disclose their identity in order to receive product recommendations on a comparator site. It is generally at the point of sale that they provide their details.

If you have any questions or would like further information regarding this submission, please don't hesitate to contact myself directly or the CPRC team at [redacted]

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.

---

[19] 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)

[20] 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)