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- Exposure Draft

7 September 2018

By email: data@treasury.gov.au

Dear Secretariat,

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- Exposure Draft.

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.

In relation to the Treasury Laws Amendment (Consumer Data Right) Bill 2018, it is CPRC's view that the Consumer Data Right (CDR) is a positive reform in the sense that it may – with appropriate protections - provide consumers with improved access to their data and give them power to direct the transfer of their data to a nominated accredited third-party. This can aid consumers to gain greater insights into their consumption, encourage greater competition between providers and enable more accurate comparisons of products and services for their needs. However, we note this reform does not prevent existing data sharing practices generally outlined in Privacy Policies or Terms of Services which allow companies (e.g. their current provider) to exchange consumer data with third parties for a variety of purposes if they fulfil their obligations under the Privacy Act. Furthermore, CDR data that is transferred outside of the CDR framework to non-accredited third parties also rely on basic privacy principles under the Privacy Act, despite small businesses not currently being captured under the Privacy Act. Analysis of the Australian privacy framework by privacy experts suggests major gaps in our data protection compared to European

standards[1]. CPRC's research also suggests a gap in privacy notice practices and data protection in Australia when compared with consumer expectations[2]. The CDR alone is insufficient in addressing privacy issues relating to existing data collection and sharing practices across the economy. Ultimately the CDR needs to be supported by economy-wide reform similar to the General Data Protection Regulation (GDPR) in the European Union (EU).

In this submission, CPRC highlights some risks identified in the Treasury Laws Amendment (Consumer Data Right) Bill 2018 as drafted that require further consideration.

Lastly, 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. This is very welcome and a positive step forward to ensure that consumers have greater transparency, control and comprehension when it comes to data ported via the CDR system. However, we continue to highlight the benefit of the implementation of economy-wide reforms in Australia alongside the introduction of the CDR. Such reforms would:

- ensure the sensible and added protections proposed by some of the CDR consent and notification requirements are also broadly applied to other data which consumers may derive benefits from.
- deliver a consistent consumer experience for consumers wishing to access or port their data to new providers or third parties.
- reduce complexity for complying businesses, enforcement agencies and consumers.
- reduce the risk to consumers of data that may be shared outside the CDR framework – for which there are currently no Privacy Act protections available for data acquired by small businesses, and no transparency, comprehension or consent requirements to ensure consumers understand the risk and implications of data sharing.

Recommendation 1: Economy-wide reform for data protection similar to the EU's General Data Protection Regulation

The introduction of the proposed CDR in the absence of economy-wide consumer and privacy protections afforded by the EU GDPR and California Consumer Privacy Act raises several complications for Australian consumers:

Complexity due to multiple frameworks

The introduction of the CDR, operating alongside the existing Privacy Act and other public sector data sharing and release legislation not only still does not provide adequate protection for the scale of consumer data collection and sharing occurring across the economy, it adds complexity and confusion for all entities in navigating and complying with the system. Some entities may even be needing to comply with three different frameworks simultaneously: the GDPR, the Australian Privacy Act, and CDR. Furthermore, the CDR Bill proposes that there may be variation in rules for different designated sectors. Having multiple systems with

[1] Esayas, S. and Daly, A. The Proposed Australian Consumer Data Right: A European Comparison. European Competition and Regulatory Law Review. 2018(2): forthcoming. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3236020 (Accessed 28 August 2018)

[2] Nguyen, P. and Solomon, L. (2018) Consumer Data and the Digital Economy. Consumer Policy Research Centre. Retrieved from http://cprc.org.au/2018/07/15/report-consumer-data-digital-economy/

varying levels of privacy safeguards is likely to introduce complexity for compliance for businesses, policymakers and regulators alike.

Introducing a GDPR-like reform in Australia will ensure that our privacy protections are at a higher standard and consistent with international standards. This is particularly important for businesses who operate in the global market. A policy analysis by Esayas and Daly (2018) comparing the Australian privacy framework with the EU suggested several shortfalls which has prevented Australia being granted data protection 'adequacy' status as a third country by the EU[3]; firstly, the Australian Privacy Act does not include small and medium enterprises with an annual turnover of less than AU$3million as liable data holders. Secondly, there are various exemptions for law enforcement and security agency activities under the Privacy Act. Thirdly, Australia is part of the Five Eyes surveillance partnership, a treaty for cooperation for intelligence with other member countries. Fourth, Australia has mandatory data retention legislation. Lastly, individuals do not have a direct means for enforcing their right under the Privacy Act in court and must contact the Privacy Commissioner to investigate their complaints.

Lastly, consumers may also be confused about what data is moving through what regulatory framework. This adds complexity and a lack of clarity about what data porting activities can be trusted as a result of the introduction of the CDR system, it also raises challenges for educating consumers about their rights.

The primary goal of implementing a CDR is for consumers to trust and use the CDR system to port their data - if that system is fundamentally flawed due to data being too easily leaked outside the protected transfer arrangements, then these gaps may undermine the intention of the reform. Consistency in consumer experience and regulatory frameworks will work to build consumer confidence, agency and control of their data to participate in data porting activities.

The UK Competition & Markets Authority[4] highlighted that in order for consumers and businesses to benefit from consumer data, consumers must be able to trust businesses so that they would continue to provide data.

They argue that consumer data can be used to support well-functioning markets if:

> *1) consumers know when and how their data is being collected and used, and have some control on whether and how they participate.*
>
> *2) businesses are using the data to compete on issues that matter to the consumer.*
>
> *3) the use of consumer data benefits both consumers and businesses.*
>
> *4) rights to privacy is protected through the regulation of data collection and use.*
>
> *5) there are effective ways to fairly manage non-compliance with regulation.*

---

[3] Ibid. Esayas, S. and Daly, A. The Proposed Australian Consumer Data Right: A European Comparison.

[4] Competition & Markets Authority (CMA). (2015). The commercial use of consumer data: Report on the CMA's call for information. Competition & Markets Authority, London, United Kingdom. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf

With the increasing collection, sharing and use of consumer data for innovation and digital transformation, it is now more important than ever to have economy-wide reform in Australia, to ensure we set up an environment for well-functioning markets into the future.

CPRC strongly recommends the Government introduce economy-wide data protection and privacy reform alongside the introduction of the CDR to improve data protection for all Australian consumers and build confidence in the CDR system.

Increased risk for data that is ported outside the CDR system

The UK Open Banking was launched on 13 January 2018 (with a roll-out completed in March 2018)[5]. The reforms were implemented within the context of privacy and consumer protections afforded by the Data Protection Act (in the UK) and Data Protection Directive (in the EU) which is now superseded by the GDPR (enforceable on 25 May 2018)[6,7]. This means that while a great deal of effort was put into developing trusted Open Banking systems to be used by consumers, the authorities assured consumers that every entity involved in Open Banking must operate under broader economy-wide data protections under the Data Protection Act in the UK, and subsequently the GDPR from May 2018[8].

In Australia, as outlined above, consumers are not yet afforded those same protections outside the CDR, for data that is 'leaked' or ported out of the Open Banking system. This in essence means that with the introduction of regimes aimed at opening up and enabling data transfers on mass, the risks to consumers increases with the velocity and volume of the transfers being enabled by the data portability system simply because data that leaks out of the system is no longer offered those same transparency and control functionality afforded by the CDR system itself. As a result, consumers would not have the same transparency, choice and control over their CDR data that might be collected, shared and used outside of the CDR system.

For data ported outside the CDR system, the existing Privacy Principles and Privacy Act apply. However, CPRC's research has shown that consumers do not believe current privacy notices and protections are adequate in aiding comprehension or choice[9]. 94% of Australian consumers who were surveyed admitted to not reading all the Privacy Policies or Terms and Conditions that apply to them in the past 12 months. Of the 67% of consumers who reported reading one or more Privacy Policies or Terms and Conditions in the past 12 months, two-thirds indicated that they still signed up even though they did not feel comfortable with the policies. The most common reason was that it was the only way to access the product or service (73%). This clearly indicates a lack of control and choice for consumers.

---

[5] Open Banking (UK). UK's Open Banking to Launch on 13 January 2018. Available at https://www.openbanking.org.uk/about-us/news/uks-open-banking-launch-13-january-2018/ (Accessed on 6 Sep 2018)

[6] Open Banking (UK). Background to Open Banking. Available at https://www.openbanking.org.uk/wp-content/uploads/What-Is-Open-Banking-Guide.pdf

[7] European Commission. General Data Protection Regulation enters into application. Available at https://ec.europa.eu/commission/news/general-data-protection-regulation-enters-application-2018-may-25_en (Accessed 6 Sep 2018)

[8] Ibid. Open Banking (UK). Background to Open Banking.

[9] Ibid. Nguyen, P. and Solomon, L. (2018) Consumer Data and the Digital Economy.

Consumers wanted more transparency and control over data collection sharing and use practices more generally:

- 95% of consumers wanted companies to give them options to opt out of certain types of information collected about them, how it can be used and/or what can be shared with others
- 91% agreed that companies should only collect the information currently needed to provide the service; and
- 92% wanted companies to be open about how they use data to assess eligibility.

Taking these factors into consideration, CPRC recommends that the Australian Government consider the benefits to the CDR system of implementing complementary reform of the Privacy Act to ensure it is fit for purpose in the new digital age and for consumers to access and share their data with confidence.

Recommendation 2: rename the Consumer Data Right to Data Portability Right

Several privacy advocates have argued that the CDR should be renamed as the Data Portability Right. There are several arguments for this:

- Considering the establishment of the GDPR in the EU, consumers may be misled in the naming of the CDR, in that it will provide the same data rights and level of protection as the GDPR when it does not. Consequently, consumers may risk sharing their data more widely with the belief that they are doing so with higher levels of protection more generally despite the CDR safeguards only applying to specified CDR datasets with accredited parties.
- A more accurate name for the reform will help to build consumer understanding and trust in the framework.
- The CDR has similar function to the Data Portability Right component (Article 20) of the GDPR, and therefore would be more accurately described as so.

CPRC supports this position and recommends the Consumer Data Right be re-named to the Data Portability Right. Though it may be worth considering a more plain language alternative description such as Transfer.

Recommendation 3: Place higher requirements on how data holders and recipients notify consumers to aid better comprehension and provide options for genuine consent, including a centralized portal for consumers to manage consent over time

Similar to the Australian Privacy Principle (APP) 1, the Bill outlines under privacy safeguard 1, that the CDR participant must have a clearly expressed and up-to-date policy about the participant's management of CDR data. The policy must contain information about the classes of CDR data held, purposes for which it will be used, how a CDR consumer is able to access the data, whether or not the participant is likely to disclose the data to accredited entities or overseas.

However, 44% of consumers surveyed in CPRC's research study did not think it was enough for companies just to notify them about data collection, use and sharing in the Privacy Policy

and Terms and Conditions. Consumers who participated in the focus group suggested that the policies were often not useful in aiding their understanding.

"I actually read the Terms and Conditions. They're written to satisfy legal requirements, not to communicate with me, and can sometimes be hard to understand."

"I skim through them, read any text that is interesting, highlighted in red, but even then, I don't understand what it means, and I don't get much out of reading it."

While privacy safeguard 5 indicates that a person that collects CDR data must take steps to notify the CDR consumer as specified under the consumer data rules (which is not yet available for review). The evidence is clear that Privacy Policies alone are insufficient as a minimum standard for notifying consumers if the goal is to aid comprehension. CPRC suggests that Treasury consider including additional minimum requirements within the Bill for data holders and recipients to provide information to consumers in ways that will aid comprehension, with specific information, unbundled options and strict conditions for consumers to provide genuine consent regarding the terms around providing their data. Rules and standards outlining how information could be displayed in a consistent format, language and visual aids, may also assist consumers in making comparisons about privacy between entities. Vague language such as "trusted third-parties or partners" should not be accepted as adequate disclosure.

Further to this, CPRC recommends that the legislation stipulate a requirement within the CDR framework to build a centralized portal for managing ongoing consent of the collection, sharing and use of their data. Professor Daniel Solove, a privacy legal expert has argued that privacy self-management alone will not provide people with meaningful control over their data and suggested that we need to find ways to facilitate partial privacy self-management, for example developing a way for people to manage their privacy for all entities rather than micro-manage their privacy with one entity at a time[10]. Similarly, the Federal Trade Commission recommended a similar model for managing data brokers access to consumer data[11]. Drawing from these examples, the CDR framework could require a portal that lists all the entities which have been 'activated' by the consumer under the CDR, where the consumer can view logs of data collection, transfers and use, and help consumers to manage their consent options over time. This mechanism will provide consumers with more meaningful control over their data and greater transparency and accountability on how the entities are operating under the CDR framework.

Recommendation 4: ensure consumers are adequately protected from non-accredited entities accessing CDR data

The CDR aims *to "give consumers more control over their information"* and place data relating to a consumer under *"strong[er] privacy safeguards once a consumer requests its transfer to an accredited recipient"*[12].

[10] Solove, DJ. Introduction: Privacy self-management and the consent dilemma. Harvard Law Review. 2013, 126(7): 1880-1903
[11] Federal Trade Commission. (2014). Data Brokers. A Call for Transparency & Accountability. Federal Trade Commission. Retrieved from https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014
[12] Australian Government. Treasury Laws Amendment (Consumer Data Right) bill 2018. Exposure Draft Explanatory Materials. Available at https://treasury.gov.au/consultation/c2018-t316972/ (Accessed 27 August 2018)

This is true to the extent that accredited data recipients will likely be required to submit to more consumer-friendly consent options, higher privacy safeguards, and face higher penalties for breaching the CDR.

Except under section 1.26 (p.9) of the Exposure Draft Explanatory Materials (EM) which explains that *"the system is flexible and may also provide via the consumer data rules, for interactions between consumers and non-accredited entities"*, thus suggesting that the system allows for the CDR data to be transferred outside the safeguards of the CDR framework.

This 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 to accessing products or services such as housing, telecommunications or utilities.

The higher penalties for misuse of data and the dual regulation (by ACCC and OAIC) to protect the CDR data will also be out of scope once the data has been provided to a non-accredited entity under the suggested Bill. 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.

EM Section 1.47 (p.12) provided an example of a circumstance where a consumer provides their CDR data to an accountant who might not be an accredited entity. CPRC recommends Treasury and ACCC to further consider how accountants could become accredited under the CDR framework. Depending on what the accreditation process might involve, we appreciate it might be impractical to require all accountants to apply for accreditation, however at the very least the CDR safeguards should still be in scope because it relates to CDR data released via the CDR framework.

Additionally, where it has been identified that the sharing of CDR data with particular classes of data recipients could put vulnerable consumers at risk of, for example predatory lending, it is recommended that these entities be required to apply for accreditation as the only way to access the information, so they must meet particular policy/practice standards, have available appropriate internal dispute processes, and also still be subject to CDR safeguards. One group identified by other privacy advocates as posing a risk to consumers are payday lenders.

Accredited recipients should still be regulated by CDR safeguards if they receive the data directly from the consumer.

Recommendation 5: Make available provisions for consumers to delete their data in circumstances when use permission has been spent or not spent

EM Section 1.219 (p.41) states that *"if a person has collected the CDR data pursuant to privacy safeguard 3 or has data that is derived from the primary data, and the person is no*

longer using the data as permitted by the consumer data rules, then the redundant data must be destroyed or de-identified according to the consumer data rules applying to the relevant type of data."

CPRC recommends that the redundant data is destroyed and not de-identified unless there are necessary grounds for keeping the data in a de-identified format. Research has shown that only few data points about an individual from other publicly available data is required to re-identify anonymised unit-level datasets with a high level of accuracy[13]. Therefore, if there is the intention to de-identify the data for other purposes, this should be based on explicit and free consumer consent.

Secondly, the right to delete data should not be limited to when use permissions has been spent. For example, if a consumer provided a CDR dataset to an entity but decided they no longer want to do business with that entity for valid reasons, they should have the option to delete the data the entity currently holds. This would help to promote consumer trust by encouraging entities to treat the data in the consumer's best interest or risk losing their business. It can be appreciated that there may be circumstances where deletion of data might not be appropriate or unfair, however this should not be a reason to disallow the right to delete for consumers altogether. CPRC recommends further consultation on how a right to deletion might appropriately be applied. Development of case studies for a variety of circumstances might assist in this process.

Recommendation 6: Minimise cost barrier for consumers in accessing CDR data

EM Section 1.51 (p.15) suggests that there would be three categories of CDR data:

1. Data that relates to a CDR consumer or has been provided by the consumer, including CDR data that relates to a person's transactions
2. CDR data that relates to a product (such as product information data like that contained in a product disclosure statement); and
3. CDR data that is derived from these 'primary' sources

EM Section 1.96 (p.21) suggests the consumer data rules may establish a fee that is payable in relation to the disclosure of certain class(es) of information under the CDR. CPRC recommends that at a minimum, CDR data provided by the consumer and CDR data that relates to a product be provided for free. Low level 'derived' data such as balances should also be available for free.

CPRC recommends at a minimum, 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 recommends providing consumers access and explanation to information that includes details of their 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 will provide consumers with greater transparency of and access to profiles, to assist consumers in checking the correctness of the derived data, challenge unfair profiling, and provide them with information

[13] 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 6 August 2018)

[14] OAIC. Accessing your credit report. Available at https://www.oaic.gov.au/individuals/faqs-for-individuals/credit-reporting/accessing-your-credit-report (Accessed 27 August 2018)

to change their behaviour for better business and consumer outcomes. Introducing fees to this class of information may act as a barrier for consumers in accessing important information that can impact their access to services and products. Any fees applied after the free quota should not be set in a way that would make the information unattainable to consumers. Furthermore, the information provided to consumer should be available in a way that is easily read and understood.

Recommendation 7: Dispute processes should be clear and resolved promptly for consumers participating in CDR

The Bill proposes that complaints would be directed to the Office of the Australian Information Commissioner (OAIC) to provide individual remedies to consumers and that the OAIC can direct external dispute resolution where relevant to the Australian Financial Complaints Authority (AFCA).

CPRC supports the 'no-wrong-door' approach where consumers access the OAIC for individual remedies and for the OAIC to facilitate connections to relevant bodies for processing external dispute resolution as appropriate. However, to provide consumers with greater confidence in the framework, CPRC recommends outlining a reasonable minimum timeframe for assigning consumers a case manager to assist them in resolving the issue. CPRC also recommends a biannual or annual evaluation of the 'no-wrong-door' approach to ensure the scheme is effective and adequately resourced for managing consumer CDR complaints.

Recommendation 8: Provide clarification on the definition of CDR consumers

In Treasury's earlier publication- Consumer Data Right Booklet[15], it was expressed that *"All customers (individuals, or small, medium or large business) will be entitled to exercise the right in relation to the classes of data covered by the right"*. There have been concerns raised that the definition of CDR consumers under section 56AF may be misinterpreted as including data holders or accredited data recipients if the CDR data is construed as relating to both the individual and the data holder/accredited data recipient. This is potentially problematic. For example, if an individual has a transaction with business X and that information is stored with bank Y, does this definition provide either business X or bank Y rights to access and port information on the individual's transaction without their consent? CPRC would like to seek clarification on what the intended scope of the definition is in the Bill.

Recommendation 9: Where possible, ensure regimes for newly designated sectors are consistent in implementing consent safeguards

CPRC is aware of discussions about potentially including energy as the next designated sector of the CDR. Given the risk energy data can have on individuals' privacy, CPRC would like to see consistent consent and privacy safeguards to be applied to this sector. This is because energy data can reveal private information about an individual's household

[15] Treasury. Consumer Data Right Booklet. Available at https://static.treasury.gov.au/uploads/sites/1/2018/05/t286983_consumer-data-right-booklet.pdf

activities, lifestyle choices,[16] and number of occupants. In general, we support consistent implementation of consent standards for newly designated sectors. This will help to support consumer trust, confidence and ongoing uptake of the CDR in other sectors. It is likely that consumers who have engaged with Open Banking may choose to participate in the CDR in other sectors by applying their understanding of how the CDR works in Open Banking. A consistent approach will aid in consumer comprehension on how to access or port their data, and the protections provided to them across sectors under the CDR.

EM Section 1.35 (pg.10) outlines that the ACCC must undertake public consultation in relation to a potential designation of a sector before providing advice to the Minister. CPRC welcomes further public consultation with stakeholders to inform how the CDR could be implemented in energy.

Thank you again for the opportunity to respond to the Bill. In particular, we have greatly appreciated the invitations to participate in both public roundtables and informal consultations which have been highly valuable in assisting us with our response to the Bill within the proposed compressed timelines. We would welcome any opportunities for further consultations and discussions throughout the coming months.

If you have any questions or would like further information regarding this submission, please don't hesitate to contact Senior Research & Policy Officer, Phuong Nguyen on 03 9639 7600 or phuong.nguyen@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.

[16] Brown, I. Britain's smart meter programme: A case study in privacy by design. International Review of Law, Computers & Technology. 2014, 28 (2): 172-184