Business Council of Australia

SUBMISSION

# Response to the Treasury Laws Amendment (Consumer Data Right) Bill 2018

**September 2018**



Business Council of Australia ABN 75 008 483 216

## CONTENTS

## ABOUT THIS SUBMISSION

The Business Council welcomes the opportunity to comment on the exposure draft for the *Treasury Laws Amendment (Consumer Data Right) Bill 2018*.

## EXECUTIVE SUMMARY

The Business Council supports giving consumers greater access and control over their personal and transaction data.

The concept of a Consumer Data Right (CDR) was recommended by the Productivity Commission and Open Banking Review, to allow consumers the right to access their personal and transaction data and request transfer of that data to third parties.

The Business Council has supported the Productivity Commission's concept and design of a CDR, as a regulatory tool that could both enhance consumers' trust and confidence in data use, and preserve the incentives for data-related business investment and innovation.

However, the exposure draft is fundamentally and unexpectedly different to the recommendations of the Productivity Commission, and other previous reviews.

As it currently stands, we anticipate the draft legislation could potentially: undermine the privacy and cyber security of consumers' data; cause tremendous confusion, uncertainty and regulatory burden for businesses – especially small and medium businesses; and put Australian companies at a competitive disadvantage, relative to their international competitors, when investing or innovating in data. Much of the risk arises from aspects of the draft legislation that go beyond the original policy objective of data portability.

Specifically, the Business Council is most concerned about:

- The expansion of the CDR to include proprietary value-added data that is not directly about a customer. Companies could be compelled to transfer commercially-sensitive information and intellectual property to their competitors.
- The establishment of a complex, brand-new privacy regime for the CDR which would operate alongside, duplicate and – in some areas – conflict with existing privacy laws. The last reform of the Privacy Act was done carefully over six years; this draft legislation tries to do the same in six months.
- The draft legislation contains unusually little detail and grants the Australian Competition and Consumer Commission (ACCC) broad powers and relatively few constraints in developing the detail after legislation has passed. The proposed delegations and powers would exceed what is needed to implement data portability.

A policy change of such magnitude should not be rushed, so risks can be fully considered. This submission proposes drafting suggestions to achieve the same policy objective – data portability – and bring the CDR back in line with the Productivity Commission's approach.

The CDR should also apply to data held by government, as per the Productivity Commission's recommendation. This is important to: protect citizens' data in their transactions with government; ensure not-for-profits and businesses can seamlessly participate in the provision of government services; and maintain incentives to design a scheme that is administratively efficient.

## KEY RECOMMENDATIONS

1. Value-added data should be excluded from the Consumer Data Right legislation.

   The exclusion should be effected through removing clauses (1b), (2) and (3) from section 56AF, and amending 'relates' in clause 4 in section 56AF to 'is about'.

   The legislation and supplementary guidance (including the explanatory memorandum) should make it clear that the legislation is not intended to capture value-added data.

2. The privacy safeguards, as currently drafted, should be substantially amended.

   Treasury should take the time to design an alternate approach to privacy that:

   - only requires compliance with one Australian privacy regime at a time.
   - does not overlap, duplicate or conflict with the Privacy Act and Australian Privacy Principles.
   - is carefully and holistically designed from the outset.
   - carefully tests and consults on any new privacy or security obligations.
   - ensures new privacy and security obligations are fit-for-purpose, proportionate and not excessive.
   - prescribes a workable approach to seeking consumer consent.
   - clearly delineates responsibilities between regulators.

3. The delegations and powers granted to the Australian Competition and Consumer Commission should be narrowed and subject to greater scrutiny and accountability.

4. The timeframe for developing and introducing the legislation should be extended, so all interested parties can properly assess the implications of the legislation and the risks and costs to consumers.

5. Treasury should undertake a comprehensive cost-benefit analysis, which considers the economic impact of the legislation (including the possible impact on future data-related investment and innovation).

6. The Consumer Data Right should be extended to include consumer data held by government agencies.

# DISCUSSION

## Why the draft legislation is important

Data is increasingly an integral part of the goods, services and business models of Australian companies – and is likely to become more so over coming years. Data use is increasingly a potential source of competitive advantage for businesses – and, as a high-skilled economy with a large services sector, the regulatory regime for data will be important in determining Australia's international competitiveness.

More extensive data use by businesses is good for consumers, delivering benefits such as more convenience, greater personalisation and lower prices.

Business Council members believe it is also imperative to earn and keep the trust of consumers – especially in how personal data is used. Businesses and governments need to work together to reduce the risk of inappropriate collection, sharing or use of data.

To this end, a well-designed CDR, as conceived by the Productivity Commission, could simultaneously enhance consumers' trust in data use, enhance convenience for consumers in porting their data, and preserve incentives for data-related investment and innovation.

The exposure draft *Treasury Laws Amendment (Consumer Data Right) Bill 2018* has moved a long way from the Productivity Commission's model.

The fundamental purpose of the draft legislation appears to have changed: from enhancing consumer trust and preserving incentives to innovate and invest, to a tool of competition policy that allows regulators broad powers to proactively shape data markets.

There is no apparent evidence to suggest data markets require new powers or tools for competition regulators beyond the existing powers and tools needed for other markets. Competition in data markets is assisted by relatively low barriers to entry[1], the constant threat of new entrants, and rapid technological change.

In moving away from the original purpose of the CDR, the exposure draft instigates a host of new concerns and risks. These are outlined in more detail below.

## Concerns with the draft legislation

There are other ways to implement the CDR, for example:

- through simple amendments to the Australian Privacy Principles; or,
- by establishing an access regime-like system that encourages direct negotiation between data holders, with potential regulatory intervention as a backstop if agreement cannot be reached.

It does not appear the advantages or disadvantages of alternative drafting approaches have been considered.

[1] It may be easier to develop a clever algorithm that establishes a solid market position than building a factory, setting up a farm or establishing a mine.

The Business Council has identified three specific areas where the draft legislation should be amended to bring the CDR back to the core concept proposed by the Productivity Commission:

1. removing value-added data (proprietary data that would include intellectual property) from the scope of the CDR.
2. reducing the complexity of the privacy regime.
3. amending the delegations and powers granted to regulators, to better reflect the principles of best practice regulation.

**Value-added data**

In this submission, value-added data is defined as data that has been subject to analysis, transformation, de-identification or aggregation to the point that it is no longer in essence the raw personal data of an individual.[2] Value-added data is proprietary data (including intellectual property) that is not directly about a customer.

Under the draft legislation, companies could be compelled to transfer value-added data to competitors.

Australians businesses use value-added data for many purposes, including to gain essential insight into consumer behaviour and respond to consumer demand, operate and run their business, and comply with regulatory requirements. Most importantly, value-added data is a key lever for businesses to respond to fierce competition.

If businesses are compelled to transfer value-added data to competitors and other third parties, they would be deprived of returns on existing investments and opportunities to gain an edge over their competitors. Competitors would receive the benefits of value-added data without needing to undertake the required investment and innovation.

The consequences would likely include:

- Discouraging investment or innovation in value-added data.
- Putting Australian companies at a disadvantage to their international competitors, who can freely innovate in their home jurisdiction (like the United States or China) and other countries who do not have such onerous requirements.
- Introducing complicated questions about the requirements of the Australian Constitution for the compulsory acquisition of property to be on “just terms”. Determining just terms for value-added data is not a simple question.

[2] We do not consider that value-added data includes: mere aggregation of personal and transaction data; cleansing of personal and transaction data; or convenient presentations of personal and transaction data.

The Productivity Commission preferred the term “imputed data” to “value-added data” because value-added data would include data that they believed should be subject to the CDR (including data that has been made machine-readable, has been aggregated or has been cleansed of errors). We prefer the term “value-added data” for the sake of clarity, however, we intend the term to have broadly the same definition as “imputed data”, as set out by the Commission.

In addition, the likely overall benefits of including value-added data would be limited:

- Value-added data is not necessary to enable data portability under the CDR.
- There has been no evidence presented that consumers desire or have any personal use for most value-added data.
- It is unlikely to encourage additional business investment or innovation. Although there would likely be some transfer of business investment and innovation (from incumbent data holders to competitors), net investment and innovation would likely decrease because of the erosion of incentives to invest and innovate.
- Additional risks to the privacy and security of customers would be introduced: for example, consumers may not be able to interpret value-added data or understand the full implications of giving third parties access to profiles of their customer behaviour. A consumer could be inadvertently disadvantaged, if a third party (for example, an insurance company) can draw unanticipated conclusions about them from their consumer profile.

None of the previous reviews into data availability or use have recommended the wholesale inclusion of value-added data in the CDR. A full list of the reviews' warnings against including value-added data are detailed in **Appendix A**, and summarised below:

- The Productivity Commission indicated value-added data should not be included in legislation.

  Value-added data was not included in the Productivity Commission's proposed legislative definition of consumer data.[3]

  It recommended value-added data should be subject to the CDR, *only if* voluntarily agreed by businesses in industry-led agreements. This was partly due to the difficulty in defining value-added data for the legislation (see specific quotes in **Appendix A**).

  Rather, the report indicates that businesses – not regulators – are best-placed to assess the value-added datasets that could be provided without discouraging investment or innovation; and there should be avenues for the voluntary inclusion of such datasets.

  Further, the Productivity Commission specifically discouraged the inclusion of data that would constitute intellectual property.[4]

- The Open Banking Review did not recommend a wholesale inclusion of value-added data in the CDR for banking[5], saying it "could make data holders less likely to make those investments [in data]".

The expansion of the CDR to include value-added data would set a broader scope of datasets than the European Union's General Data Protection Regulation, which is "arguably the most complex piece of regulation the European Union has ever produced".[6]

[3] page 203.

[4] page 17.

[5] Except for identity verification assessments for the purposes of anti-money laundering laws.

[6] The Economist, 'The joys of data hygiene', *The Economist*, 9 April 2018.

Value-added data has been included in the draft legislation without any evidence or assessment of the broader economic impact.

In some respects, the debate around including value-added data is semantic. There are many definitions of value-added data used by various stakeholders that do not necessarily align with the Business Council's intended definition. The Business Council does not consider mere aggregation, cleansing or appealing presentation of raw personal or transaction data to represent value-added data.

A preferable outcome would be to adopt the Productivity Commission's approach to value-added data: excluding value-added datasets from legislation but allow specific value-added datasets to be included in the CDR, if determined by businesses in a sector and set out in a voluntary code. Voluntary codes could be registered with – and enforced by – the ACCC.[7]

**Privacy**

The draft legislation unexpectedly contains essentially a re-write of the privacy regime (where it applies to data) through a new set of "privacy safeguards".

The safeguards would operate alongside, duplicate and – in some areas – conflict with the *Privacy Act 1988* and the Australian Privacy Principles. The ACCC would also be granted the power to create additional privacy-related rules that could apply to all or some CDR datasets. And, some Australian companies will be subject to international privacy regimes as well.

The ultimate outcome of multiple privacy regimes would be tremendous complexity and confusion for businesses (especially small and medium businesses) and consumers in understanding the privacy and security protections for CDR data.

The commencement of the CDR may risk encouraging new threats to consumers' privacy or security, including sophisticated cyber attacks and potential fraudulent or misleading conduct to obtain consumer data. Cyber security threats are an inevitable risk faced by Australian businesses who hold consumer data.

The Business Council has supported an accreditation regime to assist in managing the privacy and security risks brought on by the CDR. However, the draft legislation goes beyond to propose a complex, entirely new privacy regime on top of the accreditation regime.

It is a fallacy to believe greater regulation inherently leads to greater privacy or security for consumers. Greater complexity or regulatory burden is not good for consumers:

- In fact, greater complexity and confusion increases the risk that consumers or dataholders do not understand the regime and are exploited by ill-intentioned parties.
- The gradual commencement of the CDR and the differential regulations for different datasets will make it very hard for consumers to understand how the CDR works and assess the risks for themselves.

[7] Similar to the method by which the Australian Communications and Media Authority registers voluntary industry codes for the telecommunications and media sectors

- It also introduces tremendous confusion, uncertainty and regulatory burden for businesses. The more complex the regime, the more difficult it is for business – especially small and medium businesses – to comply with all requirements.
- Business Council members have already raised examples with Treasury where the legislation appears to inadvertently allow access to consumers' data by unauthorised third parties. There are likely other possible circumstances that could imperil consumers' privacy and security that have not yet been identified.

Similarly, overloading consumers with a greater number of complex consent requests will not improve their engagement with their privacy settings.

A wholesale re-write of the privacy regime is excessive, especially in the short implementation timeframe for the CDR.

When the Privacy Act was last reformed, it was subject to a process that lasted over six years. The current model of the MyHealth record has been under consideration since the commencement of a review five years ago, and policy makers were still not able to foresee all privacy and security concerns.

There are many new policy changes in the draft legislation's privacy safeguards that are new and have not been properly considered, including:

- The prohibition of direct marketing under the CDR (when it is explicitly permitted under the Privacy Act), under privacy safeguard 7.
- The potential requirement for businesses to expressly seek consumers' consent to provide their personal data to third parties and suppliers (such as, ICT suppliers), even when it is for the purpose of delivering the requested good or service, under privacy safeguard 6.
- The potential regulation of consumers' use of anonymity or pseudonymity, under privacy safeguard 2.
- The immediate prohibition on collecting or using existing datasets, once those datasets have been designated as "CDR data", under privacy safeguard 3.
- The potential disruption to cross-border data flows (which could potentially contravene provisions of trade agreements that prohibit data localisation measures), under privacy safeguard 8.
- The prohibition on government-related identifiers for managing consumer data, under privacy safeguard 9.
- The obligations of data holders where an inaccuracy has been identified, but a customer has not yet corrected it, under privacy safeguard 10.
- New requirements around the cyber security of CDR data, under privacy safeguard 11.

It has not been possible for the Business Council to formulate a detailed position on our preferred privacy regime in the short period allowed for consultation.

Instead, we propose a set of high-level principles by which any privacy regime that governs the CDR should abide:

- Companies subject to the CDR should only be required to comply with one privacy regime at a time.
- The privacy regime should be carefully and holistically designed at the commencement of the CDR, not set through recurrent ad hoc rule changes.
- Any new privacy- or security-related requirements should be carefully tested and subject to specific consultation and a cost-benefit analysis, prior to their commencement.

  Any new requirements beyond the Privacy Act and Australian Privacy Principles should be fit-for-purpose, proportionate, and the minimum necessary to manage risks associated with data portability.
- Requiring customer consent is a valuable tool for managing the most sensitive aspects of data use. Excessively broad requirements for customer consent can lead to "consent fatigue" and consumer disengagement with the process. There may be other ways to grant consumers' control over data without necessarily requiring their express consent (for example, requiring companies to allow consumers to opt out, if asked).
- Delineation of responsibilities between different regulators (the ACCC and the Office of the Australian Information Commissioner) should be clear.

**Delegations and powers**

The draft legislation contains unusually little detail and grants the ACCC broad powers and relatively few constraints in developing rules relating to businesses' use of data.

In consultation sessions on the exposure draft, Treasury has described the exposure draft as "framework legislation" that delegates most of the detail to the ACCC after legislation has been passed.

The resulting effect would be:

- A lack of definition relating to the nature of the CDR in any sector other than banking.
- The ACCC would be given powers to potentially regulate almost any aspect of data use (including disclosure, use, accuracy, storage, security or deletion of data).
- There are no expectations specified for consultation. There is no minimum consultation period (for example, a standard 30 days) expressed in the legislation.
- The ACCC is granted the power to make rules about how businesses appeal its own rules or decisions.
- It is not possible to properly estimate the full impact of the CDR draft legislation on investment or innovation, other than the level of uncertainty that the draft legislation would introduce to business decision-making on data. For a business weighing up

future data-related investments or innovation in data, it would be near-impossible to predict future regulatory requirements.

The amount of detail and autonomy left to regulators in the exposure draft is broad and anomalous. Taken together, the powers represent a philosophy of prescriptive and unpredictable intervention by regulators into emerging areas of innovation.

The current exposure draft would not meet standards of good regulation, such as:

- COAG's best practice guide to regulation[8], which requires that compliance requirements are clear; and government action is proportionate for the issue at hand.
- The Government's own Guide to Regulation, launched by then-Parliamentary Secretary the Hon Josh Frydenberg MP in 2014.[9] This Guide indicates all new regulation should carefully weigh up alternate options, investigate the costs and benefits, and be wary of the risk of overreach.

Our commentary about the extraordinary delegations and powers is not intended to be a criticism of the ACCC. While the ACCC would likely approach decisions about rule-making with the best of intentions, the most diligent conduct or veritable assurances from the ACCC would not eliminate the uncertainty of the draft legislation.

As a basic principle, regulators and Ministers should not be granted powers that exceed the minimum required to meet the policy objective at hand (in this case, data portability).

Greater clarity, transparency and accountability will assist to improve the quality of regulatory rules. Delegations and powers should be clear, relatively predictable and proportionate.

Ideally, the ACCC's rule-making power should be limited to advising the Minister on designating sectors (with any additional detail established through voluntary, industry-led agreements). However, if the exposure draft retains a broad rule-making power for the Minister (on the advice of the ACCC), it should be narrowed and clarified. The Business Council would recommend the following amendments:

- Introducing consultation requirements in line with accepted expectations of regulators, including a possible minimum consultation period of 30 days.[10]
- Requiring the ACCC, prior to the Ministerial designation of a sector or institution of a rule, to make its recommendations to the Minister public for a minimum amount of time (say, 60 days).
- Allowing rule-making to be initiated at the request of interested parties, but not by the ACCC itself (similar to arrangements for the Australian Energy Market Commission).
- Establishing an independent avenue for appealing ACCC rules and decisions that is not overseen by the ACCC.
- Not proceeding with a power for the ACCC to make rules relating to data use beyond what is needed to implement data portability (for example, on data deletion).

[8] Council of Australian Governments, *Best practice regulation*, October 2007, https://www.pmc.gov.au/sites/default/files/publications/COAG_best_practice_guide_2007.pdf

[9] Australian Government, *The Australian Government Guide to Regulation*, March 2014, https://www.pmc.gov.au/sites/default/files/publications/Australian_Government_Guide_to_Regulation.pdf.

[10] For example, the required processes that the Australian Energy Market Commission must follow in rule-making.

- Not proceeding with a power for the ACCC to make rules relating to privacy or security, on the assumption these are clearly set out in legislation.

**Process**

It has been challenging to properly analyse a policy change of this magnitude in the timeframe allowed.

Despite the much broader and unexpected remit of the draft legislation, the consultation period for the exposure draft legislation has been only three weeks. While it is difficult for Business Council members to ascertain all of the risks associated with this draft legislation, we imagine it has been even more difficult for small businesses, consumer groups and consumers to properly consider the breadth of the legislation's ramifications in such a short period of time.

A companion consultation paper, prepared by the ACCC on its approach to rule-making, is not being released until very shortly after submissions close on the exposure draft.

The Business Council also understands a cost-benefit analysis, currently underway, will only examine the implementation costs of the legislation and not the forgone investment or broader economic impacts.

If correct, this approach would overlook fundamental concerns about the CDR and understate the potential risks and costs of the draft legislation. Because of the increasingly importance of data in Australia's international competitiveness, the Business Council believes any legislation that could reduce Australia's competitiveness in this field (by, for example, imposing on companies operating in Australia requirements that do not exist in competitor economies) needs to be carefully considered. This consideration ought to extend to ensuring any cost benefit analysis of the proposed legislation (and any subsequent regulations) includes an assessment of any likely loss of comparative advantage or competitiveness; and the broader implications of any such loss.

For all of these reasons, the Business Council does not think it is possible to introduce a well-drafted piece of legislation for the CDR (with this scope) within Treasury's current timeframe (end 2018).

**Other**

There is no reason, in principle, why identified personal data held by governments should not be subject to the CDR as well. The Productivity Commission recommended establishing the CDR to "provide greater insight and control for individuals over how data that is collected on them is used." If this is true for businesses, it is also true for governments.

The Productivity Commission explicitly recommended that the Consumer Data Right should apply to personal data held by government agencies (excluding security-related data).

There are a number of reasons to extend the CDR to government-held data:

- The Australian Government holds a range of personal data on its citizens that could greatly enhance convenience for consumers, if it is shared with an individual's consent.

- Applying the CDR to government-held data would ensure consistency in how data is treated in sectors that involve both public and private providers.
- Not-for-profits and other businesses may face barriers to participating in the provision of government services, if government-held personal and transaction data is not transferable.
- Extending the CDR to government-held data maintains an incentive to design a scheme that is administratively efficient.

We recommend amending the draft legislation to extend the CDR to include government agencies that hold consumers' personal and transaction data, as per the Productivity Commission report.

# APPENDIX A: RECOMMENDATIONS ON VALUE-ADDED DATA FROM PREVIOUS REVIEWS

The Productivity Commission discussed in length whether value-added data should be included in the CDR. The Productivity Commission recommended that "imputed data" should be subject to the CDR, *only if* impacted businesses voluntarily agreed to include specific value-added datasets in an industry-led agreement.

The Productivity Commission said,

> "…the general intent [of the CDR] is not to automatically include genuinely transformed data. Since the extent to which transformed data is included within the scope of consumer data would be subject to an industry-specific data-specification agreement, it would seem unlikely that entities would negotiate a position that substantially reduced the value of their data analytics."[11]

Separately, the Productivity Commission recommended against including value-added data in legislation:

> "Even if desirable, it is hard to imagine how a concept like value added is able to be translated into legally effective language other than through a process of authorised negotiation."[12]

The Productivity Commission discouraged the expansion of the CDR to data that would constitute intellectual property. In fact, it indicated that requiring the transfer of data in which a third party has intellectual property rights "might prove to be an extreme step".

It recommended that "until the [CDR] is in operation and evidence of abuse, if any, of intellectual property rights emerges, the Commission prefers to allow this to be excluded from consumer data."

Productivity Commissioner Stephen King recently said:

> "Importantly, open banking does not apply to value added data, where a bank has worked with customer data creating larger data sets that, for example, allow it to better manage its whole of business risk.
>
> As the broader consumer data right spreads, the clear distinction between customer data and value-added data must be maintained to avoid creating perverse incentives."[13]

The Open Banking Review did not recommend including value-added data in the CDR for banking, except for identity verification assessments for the purposes of anti-money laundering laws. The Review's recommendation was that:

> **Recommendation 3.4 (value-added data):** data that results from material enhancement by the application of insights, analysis or transformation by the data holder should not be included in the scope of Open Banking.
>
> "If Open Banking (and broader access to data reforms) is to support the creation of an innovative Australian data industry, retaining incentives to make those investments [in value-added data] will be important. Imposing an obligation that data holders share such information with other parties (including their direct competitors), if instructed to do so by a customer, could confer an unfair

[11] page 219.

[12] page 201.

[13] S King, *Have Big Tech Platforms Got Too Much Power?,* speech delivered 31 July 2018, http://www.pc.gov.au/news-media/speeches/big-tech-power

advantage on their competitors. This could make data holders less likely to make those investments…"[14]

[14] page 38.

BUSINESS COUNCIL OF AUSTRALIA
42/120 Collins Street Melbourne 3000 T 03 8664 2664 F 03 8664 2666 www.bca.com.au