Business Council of Australia

SUBMISSION

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

October 2018

Business Council of Australia ABN 75 008 483 216

CONTENTS

ABOUT THIS SUBMISSION

This submission is the Business Council's response to the *Treasury Laws Amendment (Consumer Data Right) Bill 2018 (second stage)*. It supplements an earlier submission from the Business Council, in response to the first draft of the legislation.

EXECUTIVE SUMMARY

The Business Council supports the concept of a Consumer Data Right (CDR) but the previous draft of the CDR legislation raised, in our view, serious risks to business innovation and investment in data, Australia's competitiveness and – most importantly – the privacy and security of consumers' data.

Several amendments are proposed in the revised draft legislation, which appear to be intended to address concerns raised by the business community.

There are some welcome changes, including:

- the proposed changes to the Australian Competition and Consumer Commission's (ACCC) powers and delegations,
- the clarity around the reciprocity principle for equivalent data, and
- greater scope for CDR fees to be set by commercial negotiation rather than regulatory intervention.

Further amendments are required to address the Business Council's most pressing concerns:

- Notwithstanding amendments in the revised draft legislation, the legislation's application to value-added data requires greater clarity and precision.

  We appreciate Treasury's acknowledgement that, even though the legislation grants the Minister powers to capture materially value-added data, it is not intended to be in scope. There remains, however, the risk that the broad scope could discourage data-related innovation and investment, at the margin, because businesses who invest or innovate need to account for the possibility of inclusion of their value-added data in future.

  While the Business Council would prefer the wholesale exclusion of value-added data, we appreciate the need for legislation that can apply across the economy. If the government proceeds with capturing value-added data, there should be greater precision and clarity in the legislation. There are a number of options that could bring greater precision and clarity, including changes to the legislation, guidelines for Ministerial decision-making, or a strong indication of the intent in the explanatory memorandum or second reading speech for the legislation.

- The draft legislation has introduced some simplifications to the privacy safeguards, and narrowed the scope of privacy safeguards to data disclosure. But the privacy safeguards remain complex, confusing and a potential risk to consumers' privacy and security.

The Business Council continues to hold the view that further amendments are required to reduce the potentially major risks raised by the current draft of the legislation.

KEY RECOMMENDATIONS

1. If the government decides to leave value-added data within the scope of the legislation, there is a need for greater precision and clarity on the scope of value-added data that could be captured under the Consumer Data Right.

   Possible options for bringing greater clarity and precision could include (these are not mutually exclusive):

   - inserting greater clarity in the legislation that value-added data is not intended to be within scope, unless expressly included in a Minister's sector designation.
   - establishing guidelines around Ministerial designation of value-added datasets (that ought be regularly reviewed by the Productivity Commission).
   - emphasising strongly and clearly in the legislation's supplementary material (the explanatory memorandum and second reading speech) the intent of the legislation is generally not to capture materially value-added data.

2. Treasury should progress with its proposal to limit the rule-making power so that rules regarding use, accuracy, storage or deletion of CDR data only relate to the disclosure of CDR data. This would target rule-making towards the point of the CDR process at which there is the greatest level of risk.

3. The privacy safeguards should be amended, to provide a simpler and clearer set of protections for consumers.

4. The proposed minimum consultation requirements for designation of sectors should proceed, and should be expanded to apply to rule-making by the ACCC more generally (i.e. not just the first time the ACCC makes rules for a particular sector).

5. 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.

DISCUSSION

This submission supplements the Business Council's earlier submission in response to the first draft of the *Treasury Laws Amendment (Consumer Data Right) Bill 2018*.

In our earlier submission, the Business Council affirmed our support for the concept of the CDR, and the design of the CDR as recommended by the Productivity Commission.

However, we expressed concern that the draft legislation was fundamentally and unexpectedly different to what had been proposed in previous reviews.

Treasury should be commended for the open approach to consultation undertaken for the CDR legislation, and the short timeframe in turning out revised draft legislation that aims to address concerns raised by the business community. The Business Council appreciates the consultation paper's acknowledgement of the concerns raised.

Although some of the Business Council's recommendations have been adopted, the revised draft legislation has not made sufficient progress on our most pressing concerns.

The primary changes include:

1. Value-added data remains within the scope of the CDR, but with a number of limitations, including:
    - moving responsibility for capturing value-added data from ACCC rule-making to Ministerial designation.
    - excluding value-added data from the access and transfer requirements in the CDR, if it does not relate to a consumer and is not reasonably identifiable.
    - proposing a limitation on the areas on which the ACCC can make rules relating to use, accuracy, storage or deletion of data, so that, in respect of data holders, these rules could only apply at the point in the CDR process where data is disclosed.
2. The revised draft legislation has intended to simplify the interaction between the privacy safeguards and the Privacy Act, so the privacy safeguards would generally apply to data recipients and the Privacy Act would generally apply to data holders.
3. The revised draft legislation has been clarified to emphasise the ACCC can make rules relating to the principle of "reciprocity" (that is, if a company is receiving data under the CDR, they should be obligated to share equivalent data).
4. The powers and delegations granted to the ACCC and responsible Minister have been tightened, with greater prescription around the process that must be followed for designating a new sector under the CDR, and making rules for that sector.
5. Much greater clarity is provided in the legislation about the process for determining upfront whether the transfer of specified datasets under the CDR can attract a fee.

Many of these changes are welcome.

- The Business Council strongly supports the amendments to delegations and powers, especially the minimum consultation requirements for sector designation. The revised process now establishes greater procedural fairness and brings the legislation back in line with the delegations and powers that could be expected of regulators and Ministers.

  The Business Council recommends that the minimum consultation requirements should also apply where the ACCC makes a new rule for a sector that is already covered. Presumably, the future expansion of the CDR to any additional datasets in a sector that is already designated would need to be effected through rule-making.

  Considering the potential impact of a new rule on the use and operation of existing datasets, it would not be unreasonable to expect the ACCC would consult for a minimum period to ensure future rules are well-drafted and well-considered (except in emergency situations, as defined in the legislation).

  To ensure procedural fairness is available in all respects of rule-making, the legislation should establish an independent avenue for appealing ACCC rules and decisions that is not overseen by the ACCC.

- The Business Council welcomes the clarity around the potential to charge for datasets. We support the legislation drawing from the philosophy underpinning the

provisions in 44CA and 44ZZCA of the *Competition and Consumer Act 2010*: namely, that regulation of pricing should occur only after market participants have been unable to reach commercial agreement on their own. However, members of the Business Council have concerns that data is not sufficiently comparable to service facilities for the vertically integrated discrimination principle to be fully adopted.

We support the principles of pricing arrangements articulated in the consultation paper.

However, the Business Council's most pressing concerns around value-added data and the privacy safeguards remain. These are outlined in more detail below.

Value-added data

The CDR continues to capture value-added data[1], which is the primary example of investment and innovation in data and a key lever for Australian businesses to respond to fierce competition.

No previous review has recommended the wholesale inclusion of value-added data.[2]

We appreciate Treasury's acknowledgement that, even though the legislation grants the Minister powers to capture materially value-added data, it is not intended to be in scope. The draft legislation and consultation paper[3] has indicated an intent to clarify and tighten the provisions capturing value-added data.

However, the overly broad and ambiguous scope could discourage data-related innovation and investment, at the margin, because businesses who invest or innovate would need to account for the possibility of inclusion in future.

The Business Council would prefer the wholesale exclusion of value-added data in the legislation, and for the legislation to allow for the registration of voluntary, industry-led codes that determine the value-added datasets in scope. This would allow value-added datasets to be included in the scope of the CDR, while balancing the risks to consumers' privacy and security, business investment and innovation and Australia's competitiveness.

[1] 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. The Business Council does not consider that value-added data includes: mere aggregation of personal and transaction data; cleansing of data; or convenient presentations of data. We intend our use of the term "value-added data" to hold much the same definition as the term "imputed data", as used by the Productivity Commission.

[2] The Business Council's previous submission sets out the previous discussion from the Productivity Commission's *Data Availability and Use* report and the Open Banking Review on value-added data.

[3] *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation, Proposals* consultation paper.

However, even if one accepts the need for inclusion of some value-added datasets in the legislation, the definition remains unnecessarily broad and ambiguous for the following two reasons:

- Some types of value-added data would be captured that are not necessary for data portability and could incur unintended consequences to business investment and innovation.

  Despite the assurances that materially value-added data is generally not intended to be in scope, businesses who undertake data-related innovation or investment would need to account for the possibility that a future Minister has the discretion to capture any value-added dataset. As long as the CDR legislation contains broad discretion to capture value-added data, the CDR legislation has the potential to discourage innovation and investment in data, at the margin.

- The draft legislation excludes value-added data from the access and transfer requirements in the CDR, if it does not relate to a consumer and is not reasonably identifiable. The Business Council welcomes this change, as it excludes some datasets that are clearly proprietary, commercially-valuable and not relevant to consumers.

  However, the legislation's definition still potentially captures a broad swathe of value-added data that is not necessary for data portability. In particular, the expansion of the legislative definition from data that is *about* a customer (as per the current Privacy Act) to data that *relates to* a customer will capture data generated in the normal course of a business' operations (including value-added data like consumer behaviour insights).

  No evidence has been presented to justify the expansion, other than a desire to capture one type of dataset that was found to fall outside the scope of the Privacy Act.[4]

If the government would prefer capturing value-added data, we believe the government's objective could be delivered in a way that grants much greater precision and clarity, which would benefit businesses who are making decisions on investing or innovating in data in future.

A range of options are provided below to grant greater clarity and precision to the legislation's applicability to value-added data. These are not mutually exclusive.

- The legislation could confirm that value-added data is not intended to be within scope, unless specific datasets are expressly included in a Minister's sector designation.

- Guidelines could be prepared for Ministerial sector designations that sets out the types of value-added datasets that should or should not be included. These could be regularly reviewed by the Productivity Commission.

- A simpler legislative definition of consumer data (based on the tested scope of the Privacy Act) would be a preferable starting position for the CDR, considering the risks associated with capturing value-added data. Amending the term 'relates' in clause

[4] Ie., metadata, as determined in *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFA4

56AF(3b) to 'is about' would reflect the tested scope of personal data as currently set out in the *Privacy Act 1988* and still allow broad and meaningful datasets to be provided under the CDR.

- Finally, the legislation's supplementary material (the explanatory memorandum and second reading speech) could express clearly and strongly the intent that the legislation is generally not intended to capture materially value-added data.

Our proposed alternatives would allow the Government to deliver its objective of data portability for consumers (and account for occasional instances where value-added data is in scope of the CDR), but also address the concerns raised by businesses about the breadth and ambiguity of the draft legislation as it applies to value-added data.

Privacy

The revised draft legislation responds to stakeholder criticism about the complexity, confusion and risk resulting from essentially re-writing the privacy regime through a set of privacy safeguards that would operate alongside, duplicate and – in some areas – conflict with the Privacy Act and the Australian Privacy Principles.

The revised draft seeks to provide greater clarity around the interaction of the privacy safeguards and the Privacy Act. It proposes that most of the privacy safeguards will generally not apply to data holders and that only the privacy safeguards will apply to data recipients in respect to the data they have received.

This does not address the most fundamental concerns with the privacy safeguards for the following reasons:

- The distinction between data holders and data recipients is likely to quickly become obsolete. Shortly after the commencement of the CDR, the majority of participating companies will likely be both data holders and recipients. Even though the two privacy regimes would apply at different parts of the transfer process, firms would ultimately still be required to comply with two separate privacy regimes at the same time – potentially for the same data.
- Establishing different privacy and security standards for different CDR participants runs the risk of unintended consequences, as the same dataset is treated differently depending on relevant circumstances.
- Applying two different regimes to different parts of the transfer process *increases* the complexity and opaqueness of the privacy regime for consumers.

  It would be near impossible under this system for consumers to understand what rights and protections they can expect. This is contrary to the notion of informed consent and has the potential to harm consumers.

  A simpler and clearer privacy regime is ultimately the best way to serve the interests of consumers.
- While customer consent remains a valuable tool for managing sensitive data uses, the regime runs the risk of "consent fatigue" and consumer disengagement.

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

The amendments to the privacy safeguards in the revised draft legislation assist in some regards in clarifying and narrowing the provisions.

However, despite the amendments, the privacy safeguards remain not fit-for-purpose. There remain a series of unanswered and unclear questions about the safeguards, including:

- why the legislation introduces new requirements about anonymity and pseudonymity, which compel a CDR participant to allow consumers not to be identified (privacy safeguard 2), when the definitions of the CDR scheme are designed around data where a consumer is identified or reasonably identifiable.
- the potential disruption to supply chains or data flows due to the requirements about disclosure of CDR data (privacy safeguard 6) to suppliers or third parties in the normal course of business (for example, IT providers or call centre operators).
- the implications for cross-border data flows (which could potentially contravene provisions of trade agreements that prohibit data localisation measures), under privacy safeguard 8.
- the prohibitions on government-related identifiers for managing consumer data, under privacy safeguard 9.

Privacy regulation is an enormously complex area and careful, considered design is required to protect the privacy and security of consumers through a regime that is efficient and practical.

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.

The Business Council believes the introduction of the CDR necessitates stronger privacy and security protections for the points in the CDR process with the highest risk (disclosure or receipt of consumer data, at a consumer's request).

But there are simpler and safer ways to achieve the same objective (such as updating the Australian Privacy Principles in the Privacy Act) than the operation of multiple, concurrent privacy regimes.

As a starting point, the Australian Privacy Principles would be a tested and more considered starting point than the development of an entirely new regime. Where the Australian Privacy Principles may not entirely align with the intent of the CDR (for example, businesses are not included in the definition of consumers), amendments could be brought forward in future, once the CDR has been initially implemented.

Timeframe

The Business Council has raised concerns about the very short timeframe for developing and consulting on a policy change of this magnitude.

It has been challenging to analyse the overall operation of the CDR – and the impact of this tranche of amendments – within a short consultation period. 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.

It appears that the amendments will have a major impact on the ACCC's CDR Rules Framework, which has been available for consultation at the same time; however, it is not clear how the two processes impact each other. This is no reflection on Treasury or the ACCC; it is an inevitable hazard of progressing multiple, interlinked streams of work concurrently.

There is also no cost-benefit analysis publicly available, against which the public could assess the proposed CDR design. Without an understanding of the impact on investment or the broader economy, stakeholders' feedback cannot fully account for the entire potential impact of the CDR.

There may be additional complications from the draft legislation that could impact consumers' privacy and security that could not be fully identified or considered in the time allowed. We note, for example, that similar schemes in the United Kingdom and European Union have faced implementation issues.

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