



17 October 2018

Consumer Data Right Branch
Australian Competition and Consumer Commission

sent via email: accc-cdr@accc.gov.au

Response to the Consumer Data Right Rules Framework

To: Consumer Data Right Branch, ACCC

The Business Council welcomes the opportunity to respond to the Consumer Data Right (CDR) Rules Framework released by the Australian Competition and Consumer Commission (ACCC).

The ACCC's CDR rules are an important component of the overall design of the CDR, along with the overarching enabling legislation (currently being prepared by the Treasury) and the underpinning technical standards (currently being prepared by Data61).

The Business Council has concerns that the CDR will introduce risks to consumers' privacy and security, business innovation and investment in data, and Australia's overall competitiveness. Our preference is to resolve these concerns by amending the draft legislation through Treasury's consultation processes, however, the ACCC's approach to rule-making can assist in reducing the level of unintended risk.

We support the ACCC's general intention to prepare initial rules that are as simple and narrow as possible, to allow regulators and businesses to work through implementation issues carefully. There are additional steps the ACCC could take to minimise risks associated with the CDR:

- The scope of data for banking, and subsequent sectors, should be limited to the personal and transaction data that is reasonably required for consumers to switch providers. The ACCC should not make rules relating to value-added data¹ and broader personal and transaction data that is not required for consumers to switch providers (like metadata or geo-locational data).
- The ACCC should not make rules to require the deletion of data on request.
- The ACCC should avoid making additional privacy or security-related rules that are specific to one sector or one collection of datasets.
- The ACCC should adopt a simpler approach to the disclosure of data to suppliers or third parties in the course of normal business operations.

¹ The Business Council does 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. We intend value-added data to include data that has been materially enhanced or involves intellectual property rights. Our use of the term "value-added data" is intended to have broadly the same definition as "imputed data" in the Productivity Commission report.

- Much more careful consideration is required before expanding the CDR to vulnerable groups (such as minors) due to the risk of harm to individuals in these groups.

Our recommendations are outlined in more detail below.

Discussion

Background

As outlined in our submission to Treasury's consultation process on the *Treasury Laws Amendment (Consumer Data Right) Bill 2018*, the Business Council supports giving consumers greater access to and control over their personal and transaction data.

The Business Council has been very supportive of the original proposal in the Productivity Commission's *Data Availability and Use* report to create a CDR that enables consumers to port their data between service providers.

That said, the Business Council has concerns the exposure draft² could introduce risks to consumers' privacy and security, business innovation and investment in data, and Australia's overall competitiveness.³

Our preference is to resolve these concerns through amending the draft legislation, however, the ACCC's approach to rule-making can assist in reducing the level of unintended risk.

Although the ACCC's CDR Rules Framework paper is principally focussed on the banking sector, the CDR rules for the banking sector will set the tone for future sectors, and therefore should be assessed against the broader impact on the entire economy.

Recommendations

We support the ACCC's intention to prepare CDR rules for banking that represent a "minimum viable product", the simplest and narrowest rules necessary to enable meaningful data portability for high-priority banking products. It is prudent to commence with a narrower and simpler CDR, to minimise the risk of unintended consequences and to allow regulators and businesses to work through issues before implementing a more ambitious scope.

The Business Council agrees with many of the proposals in the Rules Framework, including:

- excluding large business customers
- excluding former customers
- excluding offline customers
- leaving identity verification assessment (performed for anti-money laundering or counter terrorism purposes) out of the initial rules.

There are additional steps the ACCC could take to minimise risks associated with the CDR. The Business Council makes the following recommendations:

² Originally released in August 2018; revised version released in September 2018.

³ These are detailed more in our submissions to the exposure draft consultation processes, available at the Business Council's website.

- The scope of data should be limited to the customer’s personal and transaction data that is reasonably required for consumers to switch providers. Value-added data, and a broader definition of personal and transaction data (to capture metadata or geo-locational data), should be excluded from the ACCC rules.⁴

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

If the scope of value-added data is too broad, consumers may be able to transfer value-added data that has little personal value but significant commercial value. Companies who have already invested or innovated in value-added data could be deprived of returns on existing investments and opportunities to gain an edge over their competitors, as competitors receive the benefits of value-added data without needing to undertake the required investment and innovation.

The consequences could include:

- Discouraging investment in value-added data, at the margin.
- Stifling data-driven innovation and productivity.
- Putting Australian companies at a disadvantage compared to their international competitors, who can freely innovate in their home jurisdiction (like the United States or China) and other countries that do not have such onerous requirements.

There has been no evidence presented that consumers desire or have any personal use for value-added data.

For these reasons, none of the previous reports by the Productivity Commission or Open Banking Review have recommended the wholesale inclusion of value-added data.⁵

Even if the final legislation allows for the institution of rules relating to value-added data, we would recommend the ACCC undertake a comprehensive assessment of the costs and benefits (including the impact on investment and innovation), prior to instituting any rule relating to value-added data or broader datasets. We believe a comprehensive cost-benefit analysis would find that the risks of a broader data scope would substantially outweigh the benefits.

The ACCC has also sought views on whether metadata or geo-locational data should be within scope of the first rules for the banking sector.

The complexity, cost and risk of expanding the CDR to these datasets should not be underestimated. Expanding the CDR scope to metadata or geo-locational data would extend the CDR far beyond a “minimum viable product”.

- The ACCC’s rules should not require data to be deleted or de-identified on request.

The Rules Framework seeks views on whether to grant consumers the right to instruct the deletion of data.

⁴ The Productivity Commission reflected on this matter in its report: “The overarching outcome to be legislated is that the scope of consumer data in an industry is that which is sufficient to generate a competitive offer for an individual’s custom from another provider. In other words, the type of data held on an individual or SME that a competing or complementary service provider would themselves need, and reasonably expect to obtain, in seeking to provide a competitive offering.”

⁵ The Open Banking Review only recommended including one value-added data set: identity verification assessments undertaken for anti-money laundering or counter terrorism purposes. The Review only recommended including these assessments if the anti-money laundering legislation was amended to allow data recipients to rely on the outcome of assessments.

A rule requiring companies to delete or de-identify a customer's personal or transaction data on request would be complex, difficult to enforce (in light of the global nature of data flows), and overly burdensome.

Consumers will have various means to exert control over what CDR data companies hold: the Australian Privacy Principles already require companies to destroy or de-identify personal information that is no longer needed for its original purpose.

The CDR will also introduce new, different requirements that grant customers greater control and assurance over their data, including new requirements around seeking consumer consent and ensuring the integrity of CDR data.

For these reasons, a right to deletion was not recommended by the Productivity Commission or Open Banking Review.

- The ACCC should aim not to create any privacy or security-related rules that are specific to one sector or collection of datasets.

In our submission on the exposure draft, the Business Council raised concerns about the complexity of the draft privacy safeguards. Greater complexity or onerousness ultimately does not serve customers well, because it increases the level of risk to consumers and makes it very hard for them to understand the CDR or assess the risks for themselves.

The Business Council recommends that companies subject to the CDR should only be required to comply with one privacy regime at a time. Preferably, the CDR would be covered by one clear, fit-for-purpose privacy regime, instituted through legislation.

While the design of the final legislation is outside of the ACCC's control, the complexity of the scheme would be exacerbated if the ACCC instituted additional privacy or security requirements on top of the Privacy Act, the Australian Privacy Principles, and the privacy safeguards in the CDR legislation.

We believe the CDR should attract additional privacy or security requirements; but we believe that these should be established in a carefully and holistically designed set of legislative requirements, rather than complex and ad hoc rules.

- The ACCC should consider a simpler approach to disclosure of data in the normal course of business operations (ie. not at a customer's request, but provided to suppliers or third parties).

Where use of suppliers or third parties involves global data flows, the ACCC's proposed approach could potentially disrupt or complicate the normal course of business operations (for example, the requirement of express consent before CDR data is provided to an offshore provider).

The Privacy Act applies a different approach, which allows the provision of information to offshore providers as long as they meet the standards set in the Privacy Act.

Adopting a different approach under the CDR rules could require material changes to business processes or systems.

- We discourage the expansion of the CDR to vulnerable groups (such as minors) without carefully designing measures to minimise the risk of harm to individuals in these groups.

On broader issues, we also recommend the ACCC prepare an overarching Rules Framework that establishes the principles and process that the ACCC will follow when making any CDR rule, to provide greater predictability to businesses who may in future be captured by CDR rules after a sectoral designation. This Rules Framework should be ongoing and binding. Although the current consultation paper is entitled a Rules Framework, it is primarily focussed on a set of draft rules for the banking sector.

Finally, the Business Council remains of the view that it will be challenging for a CDR that has been comprehensively considered to be finalised within the current timeframe. There are multiple, complex processes by the Treasury, ACCC and Data61 simultaneously underway to design different elements of the CDR. It has been difficult to assess the impact of each component within relatively short consultation timeframes.

Thank you again for the opportunity to participate in the consultation process.

Further questions can be directed to myself, or Mr Josh Machin, Director, Policy at [REDACTED]

Yours sincerely

A handwritten signature in black ink, appearing to be 'A Boyton', with a long horizontal flourish extending to the right.

Adam Boyton
Chief Economist