TELSTRA CORPORATION LIMITED

Submission to Treasury consultation on

Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation

Public version

12 October 2018

CONTENTS

EXECUTIVE SUMMARY		**3**
01	**Value-added data**	**4**
02	**Interaction of the Privacy Safeguards and the Privacy Act**	**6**
03	**Recognition of alternative frameworks**	**8**
04	**Putting customers at the centre of the CDR**	**9**
05	**Other issues**	**10**
5.1.	Definition of "CDR consumer"	10
5.2.	Extension of the ACCC's section 155 powers	10

EXECUTIVE SUMMARY

Telstra welcomes the opportunity to comment on the *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation*.

As discussed in our response to the first round of consultation on the Consumer Data Right (**CDR**) Bill, we are generally supportive of reforms aimed at improving data availability and use in Australia. Data reforms of this kind have the potential to promote consumer interests, and drive competition and innovation, as well as helping to establish and normalise a safe and trusted environment in which data is used to benefit consumers and the economy.

In its second round of consultation on the CDR Bill, Treasury is seeking views on five proposals designed to address concerns raised by interested parties about the first draft Bill. These relate to:

- derived data;
- privacy;
- reciprocity;
- consultation requirements for sectoral designation and rule-making; and
- charges for access and use of data.

Treasury's proposals go some way towards addressing issues raised by stakeholders about the first draft CDR Bill. In particular, we are very supportive of the proposal to introduce minimum consultation requirements prior to a sector being designated or rules being made. Given the importance of sectoral designation and rule-making, appropriate consultation processes and timeframes are critical.

In the remainder of this submission, we address the following aspects of the second draft CDR Bill in more detail:

- the inclusion of value-added data within the CDR regime;
- the parallel privacy regime contemplated by the CDR Bill;
- the need for express recognition of alternative frameworks that achieve the objectives of the CDR;
- the importance of putting customers at the centre of the CDR; and
- several other issues, including the broad definition of "CDR consumer", and the proposed extension of the ACCC's powers under section 155 of the *Competition and Consumer Act 2010* (Cth).

We do not propose to make any comments about Treasury's proposals regarding reciprocity or charges for access and use of data.

01 Value-added data

In our submission to Treasury regarding the first draft CDR Bill, we set out in detail our position that value-added data should not be included in the CDR regime. We provided two main reasons for that position:

- **Value-added data is not required to facilitate competition**:

  The data required to achieve the objectives of the CDR is, at most, raw transaction data (which accredited data recipients can then use to carry out their own derivations as needed).

  To the extent that companies generate value-added, inferred or derived data, they do so through intellectual, technological and financial investments and for a range of purposes such as improving products and services, identifying new product opportunities and markets, or to achieve business efficiency gains that lower costs. Ultimately the benefits resulting from these investments in data and its analysis accrue to consumers through more competitive offerings, or new products and services better suited to the needs of consumers.

- **A requirement to disclose value-added data will reduce business investment in data and analytics:**

  Forced disclosure of value-added data (including derived and inferred datasets) to competitors, even on a "per consumer" basis, risks undermining investment by businesses in data and its lawful analysis for competitive commercial purposes.

In addition, value-added datasets will vary over time, so a broad definition of CDR data covering all derivations of designated datasets will have an increasingly uncertain scope over time.

Treasury's proposed amendments to the draft Bill help address these concerns by moving to the Ministerial level the decision about the scope of data which customers can ask to be disclosed under the CDR regime. In particular, Treasury is proposing to:

- limit the ACCC's rule-making power so, where information relates to a consumer, the access and transfer right will only apply to information in the designation instrument; and
- require the Minister, in making a designation, to consider the likely effect on any intellectual property in the information covered by the instrument.

In addition, Treasury's document outlining this proposal states: *"Intellectual property remains potentially within scope to address potential loopholes and uncertainty that could otherwise arise. However, it is not anticipated that it would be likely for any intellectual property to be designated for most sectors".*[1]

Treasury's proposed amendments, coupled with its acknowledgment that it is unlikely any IP would need to be designated for most sectors, are an improvement on the first draft Bill. However, more detailed guidance should be provided about the circumstances in which the Minister may or may not designate derived data under the CDR regime. It is not clear what "potential loopholes and uncertainty" the Minister may be seeking to address through designating derived data. Yet there is a real risk that, if the

[1] Treasury, *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation*, Proposals, 24 September 2018, page 5.

legislation leaves open the future possibility of including value-added data, incentives for business to invest in data and analytics will be reduced.

It would be preferable to identify, as specifically as possible, the types of derived data sets which may by captured by the CDR regime, and otherwise exclude value-added data from the scope of the CDR. Alternatively, the legislation should exclude value-added data, unless that exclusion would undermine the transfer of the necessary raw data to enable the framework to function. This would have the effect of preventing loopholes, but without including in the CDR legislation an overly broad power to designate or make rules about value-added data.

02 Interaction of the Privacy Safeguards and the Privacy Act

In our submission to Treasury on the first draft CDR Bill, we expressed our concern that having parallel privacy regimes in the *Privacy Act 1988* (Cth) (**Privacy Act**) and the *Competition and Consumer Act 2010* (Cth) (**CCA**) would be difficult to work with for data holders, accredited data recipients, and consumers. Our view was that the relationship between the Australian Privacy Principles (**APPs**) and the Privacy Safeguards, and the way in which they work together, was unclear and would likely give rise to questions and uncertainties about which regime applies when, and the differences between the two.

Treasury has sought to clarify the interaction between the APPs and the Privacy Safeguards by, for example, proposing that most of the Privacy Safeguards will not apply to data holders, and that only the Privacy Safeguards (and not the APPs) will apply to data recipients in respect of CDR data they have received.

While Treasury's proposals clarify the *application* of the APPs and the Privacy Safeguards to the various CDR participants, we remain concerned that, *in practice*, implementation of parallel privacy regimes is likely to be difficult. For example, we expect entities participating in the CDR regime will, in many cases, be participating as data holders and accredited data recipients, potentially in respect of the same consumer at different times. This is likely to give rise to complexities with implementation, and confusion on the part of consumers considering participating in the CDR regime. This is particularly so in the telecommunications sector, which is already subject to a complex set of laws and regulatory requirements governing the collection, handling and storage of data – including a telco-specific privacy regime in Part 13 of the *Telecommunications Act 1997* (Cth).

We fully acknowledge the importance of ensuring privacy is protected. We remain concerned the CDR regime will not achieve wide adoption without consumer confidence in data privacy, and confidence will be very difficult to establish, or could simply be lost, under a regime that is complex to understand and implement.

It seems much of the complexity and many of the issues around privacy arise because the CDR framework focuses on data holders transferring CDR data to accredited data recipients. This could be avoided if the draft legislation recognised alternative (and in some cases existing) frameworks whereby suppliers provide data to consumers, who then have complete control over who they provide that data to. This would also be consistent with the objectives of the CDR regime, which Treasury summarised most recently in the following terms:

> *"The primary aim of the Consumer Data Right (CDR) is to give consumers the ability to access more information about themselves, and about their use of goods and services, in a manner that allows them to make informed decisions about both themselves and their participation in the market. By doing so, the CDR aims to increase competition in any market, enable consumers to fairly harvest the value of their data, and enhance consumer welfare. This should be done in a manner that fairly considers incentives for all participants."*[2]

We are concerned Treasury's proposal to address the privacy issues raised during the first round of consultation does not adequately deal with the complexities of implementing parallel privacy regimes.

[2] Treasury, *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation*, Proposals, 24 September 2018, page 2.

Nor does the proposal seem to deal with the fact that these complexities could be avoided – to the benefit of all CDR participants – by placing consumers more firmly at the centre of the CDR regime in terms of their direct access to and sharing of their own data. Indeed, the complexities associated with the introduction of parallel regimes may well compromise the very privacy the regimes seek to protect.

We would recommend the legislation enable the CDR framework to be satisfied by data holders providing data directly to customers (rather than to data recipients directly), or that there is further clarification and streamlining of the privacy regime to remove complexity. For example, the CDR Bill could focus on ensuring there are appropriate privacy and security protections around the disclosure and transfer processes for CDR data, and greater reliance could be placed on compliance with the APPs as far as possible in respect of CDR data held by data holders and accredited data recipients.

03 Recognition of alternative frameworks

The telecommunications sector already incorporates a range of mechanisms for access to, and sharing of, data:

- Suppliers offer plans for broadband and mobile services that make the customer's choice between providers very simple. For example, many suppliers offer plans with simple monthly fees, often without the requirement to contract.
- Customer bills already detail the user's consumption (calls, SMS, and data usage) at a granular level, and this information can be taken or forwarded to other suppliers in the industry for the purpose of obtaining a competitive quote.
- Beyond this, customers often have access to more information about their telecommunications consumption than their providers do. For example, mobile phones store calling histories for calls made on the provider's network, and via apps like WhatsApp and Viber, as well as data consumption (which may be on a "per app" basis). This level of detail far exceeds information that could be gathered by a service provider for compliance with the CDR regime, given the service provider has no visibility of calls / messages from OTT applications or of data consumption at a "per app" level.
- In addition, the telecommunications sector already has mature processes and regulation facilitating switching from one supplier to another, including a range of ACMA determinations underpinning a strongly competitive market in which switching between competitors is high. For example:
    a. The Telecommunications Numbering Plan requires all carriers and carriage service providers to implement number portability for fixed and mobile services. This means the removal of technical barriers to customer switching – a principal objective of the CDR regime – is already satisfied within the communications sector.
    b. The Telecommunications Consumer Protections Code requires suppliers to provide critical information summaries (short but detailed information about plans) to customers at the time of sale, and contains standardised bill inclusion requirements.

We think it is important that the CDR legislation includes an express requirement for the Minister and the ACCC to consider pre-existing industry regulation that meets the objectives of the CDR regime, along with technical alternatives (that may exceed the granularity of information able to be collected by a service provider).

The Explanatory Memorandum notes that, under section 56AD(1)(c), the Minister may consider any other relevant factors in deciding whether to designate a sector, and that this *"could include considering a consumer's existing access to a particular data set"*.[3] In addition, the Minister is required to consider the regulatory impact of designating a sector, which would require an assessment of the net benefits of designation.[4] However, for the reasons outlined above, we believe a separate requirement to consider existing regulation and processes which facilitate data portability and customer switching is important.

[3] Explanatory Materials, *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation*, page 6.
[4] Explanatory Materials, *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation*, page 6.

04 Putting customers at the centre of the CDR

We believe there is a simple way of addressing the privacy issues discussed in section 2 of this submission, and of directly recognising alternative ways of achieving the objectives of the CDR regime as discussed in section 3.

In essence, that simple way would put consumers (rather than accredited data recipients) at the centre of the CDR, and would allow data holders to provide data directly to consumers to satisfy the requirements of the CDR. This would give consumers the power to supply their data to other providers (or just to use it themselves).

This would not require much effort from the customer – for example, any future use of the data could be automated by apps on their phones. Indeed, in the telecommunications sector, such an app could make use of more data on a customer's phone than any one data holder would have access to.

We note this is similar to the framework developing with respect to Facebook and Google, whereby customers are able to download their data for their own use, and to provide that data to other parties as they see fit.

05 Other issues

5.1. Definition of "CDR consumer"

In the revised draft of the CDR Bill, the definition of "CDR consumer" has been amended to make it clear the term refers to an identifiable or reasonably identifiable person to whom the CDR data *relates* because of the supply of a good or service either to the person or an associate of the person.

The Explanatory Materials – for the first draft Bill and for the revised provisions – indicate the term "relates to" is a broader concept than information "about" an identifiable or reasonably identifiable person under the Privacy Act, and is intended to capture, for example, meta-data of the type found not to be about an individual in *Privacy Commissioner v Telstra Corporation Limited*.[5]

As stated in our submission to Treasury about the first draft Bill, the boundaries of the concept "relates to" are unknown and potentially far-reaching, and using this term in the CDR legislation is likely to give rise to a range of potential issues:

- First, it is not clear why using the term "relates to" rather than "about" will help achieve the stated objectives of the CDR regime. In particular, it is not apparent why *"meta-data of the type found not be 'about' an individual in* Privacy Commissioner v Telstra Corporation Limited*"* would be relevant to a customer considering switching away from their existing telecommunications provider.
- Secondly, including meta-data within the scope of the CDR risks introducing additional privacy and security issues into the regime. For example, account-level meta-data could potentially capture password changes on an account.
- Thirdly, meta-data is, in our view, proprietary data, and should generally be excluded from the scope of the CDR regime consistent with the reasons discussed in section 1 of this submission, and in our previous submissions on the government's proposed data reforms.

5.2. Extension of the ACCC's section 155 powers

We remain concerned about the proposal to allow the ACCC to delegate its section 155 powers for the purposes of the CDR regime. In particular, we do not believe it is appropriate to empower the ACCC to delegate its section 155 powers to any "other person" (as is proposed by the addition of section 26(5) of the CCA). Given the coercive nature of section 155 notices, the potential impact on notice recipients, and the consequences for non-compliance, we consider that the grant of these types of powers should generally be left to Parliament, not delegated by one agency to another.

[5] Explanatory Materials, *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation*, page 11.