TELSTRA CORPORATION LIMITED

Submission to OAIC consultation on

Draft CDR Privacy Safeguard Guidelines

Public version

20 November 2019

01 Introduction

We welcome the opportunity to comment on the Consumer Data Right (**CDR**) Draft Privacy Safeguard Guidelines (the **Guidelines**). We have previously expressed our in-principle support for greater availability and use of data in Australia, balanced with the need to protect the privacy of Australians. In doing so, we focused on the proposed introduction of a CDR as a way to promote consumer interests and help drive competition and innovation across the economy. We believe these data reforms could help establish and normalise a safe environment that is trusted by consumers, within which private and public enterprises can use data to the benefit of consumers and the economy.

On the whole, the Guidelines provide clear and helpful instructions for CDR participants who have to navigate the overlapping Australian Privacy Principles[1] and CDR Privacy Safeguards,[2] which have the potential to cause confusion given the similarities and differences between the two sets of requirements. We commend the OAIC for creating Guidelines that explain how and when each piece of legislation applies to each CDR participant.

Therefore, our brief submission offers a few minor suggestions to improve the Guidelines' useability:

- **Section 2**: explores the practicalities of complying with APP 1 and Privacy Safeguard 1 and suggests the OAIC create a template that would provide consumers (CDR and non-CDR) with a familiar format;
- **Section 3**: explores two scenarios, one of which is unique to the telecommunications sector, where we recommend the Guidelines (and CDR Rules) would benefit from further examples; and
- **Section 4**: identifies one potentially unclear aspect in Chapter C of the Guidelines.

02 Publishing policies on handling data

We have previously noted[3] the overlapping Australian Privacy Principles (APPs) and Privacy Safeguards have the potential to cause confusion for CDR participants, including CDR consumers. For example, APP 1 and Privacy Safeguard 1 both require entities to have a clearly expressed and up-to-date policy about how they manage customers' data, and we foresee that Australian businesses may have different approaches to how they manage customer data depending on whether the data arrives under the CDR regime or outside of it.

For example, an Accredited Data Recipient (**ADR**) might have no reason to disclose certain information received under the CDR regime to third parties (such as contractors or subcontractors). However, in order for an ADR to provide goods and services to a customer, it might need to disclose the same customer information (e.g. customer name, address, date of birth, etc.) received outside the CDR scheme to third parties such as call-centre facilities and data warehouse facilities including off-shore data warehouses.

This issue arises when considering a number of the APPs and Privacy Safeguards, including APP 6 versus Privacy Safeguard 6 on disclosure, APP 8 versus Privacy Safeguard 8 on overseas / cross-

1 https://www.oaic.gov.au/privacy/australian-privacy-principles/
2 Division 5, Part IVD, Competition and Consumer Act.
3 Telstra submission to Treasury Laws Amendment (Consumer Data Right) Bill 2018, available at https://treasury.gov.au/sites/default/files/2019-03/t329531-Telstra.pdf. Section 05.

border disclosure of information, and APP 11 versus Privacy Safeguard 12 which require the de-identification or destruction of redundant data.

Australian businesses participating in the CDR regime will need to explain to consumers how, where and when they disclose information to third parties. We propose that it would be beneficial to CDR consumers if a consistent format were available for Australian businesses to use as they attempt to explain the different treatment of often the same data under the different regimes. We propose it would be helpful for the OAIC to provide a template for businesses to use in meeting their obligations under APP 1 and/or Privacy Safeguard 1 that enables a consistent and familiar format for CDR and non-CDR consumers to follow.

03 Telecommunications scenarios

The Guidelines will need to be revised as additional sectors are brought into the CDR regime. For example, the sections on eligible CDR consumers[4] are predicated on Schedule 3, Part 2, clause 2.1 of the CDR Rules, which only covers the banking sector. These sections of the Guidelines will need to be updated to reflect the eligibility criteria for other sectors as they are designated over time. As a part of those updates, we propose it would be helpful to include additional examples to cover the following scenarios, which should also be addressed in the CDR Rules themselves.

3.1. Employer supplied service

The first scenario is where an employer supplies an employee with a telecommunications service, for example, a mobile phone. The CDR regime is strongly predicated on express consent from the CDR consumer to underpin privacy protection when data is being sent by a Data Holder (**DH**) to an Accredited Person (**AP**) or ADR. In the employer/employee context, there are two parties with a potential interest in providing consent. One is the employer who pays for the service and whose name the service is likely to be in, and the other is the employee who makes phone calls and uses data, and is therefore the person the CDR data is 'about'. We acknowledge that as a result of itemised billing records, the employer would already have access to detailed call records; however, the employer having access to this information is very different from consenting to that information being handed over to a third party.

We note the CDR rules for banking have deliberately addressed joint accounts[5] under Schedule 3, as these services are peculiar to the banking sector. When the time comes, it will be important for the CDR rules for the telecommunications sector to address employer / employee scenarios, which would then need to be reflected in a future version of both the CDR Rules relating to the Privacy Safeguards and the Guidelines.

3.2. Minors, the elderly and vulnerable customers

The second scenario we believe deserves specific attention relates to a telecommunications service purchased on behalf of a minor or an elderly relative. In the case of a minor, for the banking sector we note the CDR eligibility criteria[6] prevent people under the age of 18 from being CDR consumers. This implies it is possible to identify the age of the consumer, which may be the case for banking. In the telecommunications sector, we observe that for minors, a (mobile) phone service is often purchased by a

4 Draft Privacy Safeguard Guidelines, Chapter B, sections B.51-B54.
5 CDR Rules, Schedule 3, Part 4.
6 CDR Rules, Schedule 3, Part 2, section 2.1(2)(a).

parent or guardian in their name, and then is used by the minor. In such cases, the telecommunications service provider has no visibility of the age of the actual user of the service.

In the case of an elderly relative or any other party where a service is purchased on their behalf (e.g. vulnerable, disabled, etc.), we observe neither the CDR rules nor the Privacy Safeguards currently address this for the banking sector. Nevertheless, the same challenge in identifying that the actual user is different to the account owner exists, and yet any of these scenarios (minors, elderly, vulnerable or disabled) potentially have privacy implications where the person providing the CDR consent and/or the authorisation to transfer CDR data is not the actual user of the service.

We believe it would be helpful to CDR participants if the CDR rules and Privacy Safeguards clarified who is able to provide CDR consent in the scenario where the user of a service (banking product, telecommunications service, etc.) is different from the person who may notionally be in a position to provide CDR consent and/or authorisation.

04 Flow diagram in Chapter C misses authorisation

The flow diagram in Chapter C (p.5) is a helpful way to visualise the steps involved in two key CDR processes: firstly, obtaining express consumer consent for the collection and use of CDR data; and secondly, an AP making a valid consumer data request on behalf of the CDR consumer.

In the second example, the light-grey shaded bar towards the bottom of page 5 simply shows the DH sending consumer data to the ADR without further steps. We suggest that this simplification of the process has the potential to be unclear, as the DH cannot proceed to send the data to either an AP or ADR without first obtaining **authorisation** from the CDR consumer pursuant to Division 4.4 of the CDR Rules. Indeed, this authorisation step is noted in Chapter B paragraph B.134 of the Guidelines.

We propose the light-grey bar should be amended to say "*Data holder obtains CDR Consumer Authorisation and sends data to accredited data recipient*" (underlined text to be added as clarification).

Chapter C might also benefit from some explanatory paragraphs referencing Division 4.4 of the CDR rules, similar to those referencing Division 4.3 on Consent to help explain the obligations on DHs to obtain authorisation.