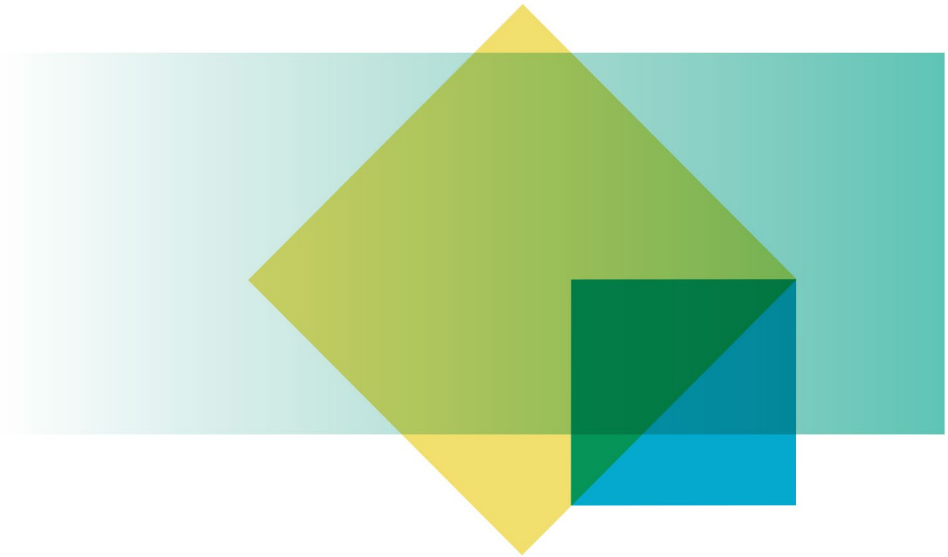
Australian Government

Office of the Australian Information Commissioner

Report on the draft Consumer Data Right (Telecommunications Sector) Designation 2021

A report by the Australian Information Commissioner, pursuant to section 56AF of the *Competition and Consumer Act 2010*



Angelene Falk

Australian Information Commissioner and Privacy Commissioner

23 December 2021

OAIC

Contents

Introduction

I welcome the opportunity to provide this report on the Consumer Data Right (Telecommunications Sector) Designation 2021 (the draft instrument). The draft instrument and its explanatory material are available at (https://treasury.gov.au/consultation/c2021-224994), having been published by the Department of the Treasury (Treasury) for a period of public consultation from 23 November – 13 December 2021.

As Australian Information Commissioner (Information Commissioner), this report is produced in fulfilment of my obligation under s 56AF of the *Competition and Consumer Act 2010* (CC Act). Section 56AF requires the Information Commissioner to:

a) analyse the likely effect of making the draft instrument on the privacy or confidentiality of consumers' information, and
b) report to the Minister about that analysis.

As required by s 56AF(2) of the CC Act, this report will be published on the Office of the Australian Information Commissioner (OAIC) website. This report also constitutes evidence of the consultation required by section 56AD(3) of the CC Act, which provides that the Minister must consult the Information Commissioner before making an instrument designating a new sector as subject to the CDR.

If made, the draft instrument would have the effect of making telecommunications a 'designated [CDR] sector' (see s 56AC of the CC Act) and enlivening the ability to make rules allowing for the sharing of designated telecommunications datasets pursuant to the CDR (see Division 2 of Part IVD of the CC Act). The instrument does not, without applicable rules (CDR rules), allow for the sharing of telecommunications data pursuant to the CDR. The CDR rules can regulate the sharing of designated data to the extent that it is held by a 'data holder'. [1] The draft instrument provides that carriers and carriage service providers (CSPs) are data holders for designated telecommunications data.[2] New or amended CDR rules would need to be made to allow the sharing of telecommunications data that falls within the scope of the draft instrument.

In producing this report, I have had the benefit of reviewing publicly available submissions to the July – August 2021 consultation on the possible designation of telecommunications as a CDR sector (the sectoral assessment consultation).[3] My submission to that sectoral assessment consultation is available on the Treasury website.[4] I have also reviewed the sectoral assessment report produced pursuant to s 56AE of the CC Act (the sectoral assessment report) and the accompanying privacy impact assessment (PIA).[5]I have not considered datasets which are outside the scope of the draft instrument, but which had previously been considered during the sectoral assessment consultation. OAIC staff have also had ongoing engagement with Treasury to ensure a common understanding of the matters at hand and applicable privacy and confidentiality implications. OAIC staff attended

[1] See ss 56AC(2)(b), 56AJ, 56BC of the CC Act.

[2] See clause 5 of the draft instrument.

[3] Available at https://treasury.gov.au/consultation/c2021-198050-tc.

[4] Available at https://treasury.gov.au/consultation/c2021-198050-tc.

[5] Available at https://treasury.gov.au/publication/p2021-225262.

roundtables with government and industry representatives on 7 and 8 December 2021 and have been privy to feedback industry provided to the consultation process.

I have conducted my 'analysis [of] the likely effect of making the instrument on the privacy and confidentiality of consumers' information' (per s 56AF, CC Act) by reference to whether the applicable privacy and confidentiality implications are reasonable, necessary and proportionate. As such, my analysis has been informed by a variety of factors, including:

- the inherent sensitivity of telecommunications data and the importance of robust regulation to ensure such data is handled appropriately[6]
- the potential benefits of expanding the CDR to telecommunications – including increased innovation and competition
- the role of the designation instrument in the broader CDR framework, noting that the ultimate impact of the designation instrument depends on provisions of the CC Act and CDR rules which govern the handling and protection of designated data
- community expectations around the handling of telecommunications data, noting the particular importance of robust privacy safeguards in the context of evidence that the community may trust telecommunication providers less than other sectors (such as financial institutions) with respect to the handling of personal information[7]
- the importance of ensuring the CDR is easily understood and operationalised, so as to protect against risk of error in the application of privacy safeguards and protections, and
- the benefits of a flexible and future-focussed CDR which can readily adapt to embrace new and emerging use-cases, supported by robust privacy protections and safeguards.

Having considered these factors, I have concluded that, on balance, the privacy and confidentiality impacts of designating telecommunications as a CDR sector can be appropriately mitigated and managed within the CDR framework. My report makes recommendations to this effect, with the aim of ensuring that the identified privacy and confidentiality impacts of designation (in the context of the broader CDR framework) are reasonable, necessary and proportionate.

I also note that a further PIA will be conducted at the rule-making stage (see page 16, sectoral assessment report), and that I will be required to analyse any new CDR rules before they are made (s 56BR, CC Act). At that point, I will consider and make any further recommendations to ensure the appropriate protection of privacy and confidentiality in the CDR's operation in the telecommunications sector.

[6] See in particular pages 4 – 5 of my submission to the sectoral assessment consultation process, available at https://treasury.gov.au/sites/default/files/2021-11/c2021-198050-tc-oaic.pdf.

[7] See OAIC's 2020 Community Attitudes to Privacy Survey (especially page 55), available at https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf.

Summary of recommendations

Recommendation 1
That the draft instrument be amended to clearly exclude the following information from designation, and that the exclusion of these data types be highlighted in the explanatory statement:

a) the substance of communications
b) information relating to the destination of communications – including information about the recipients of communications (unless the recipient is the CDR consumer or their associate) and web browsing history records
c) data relating to 'over-the-top' services
d) information about a person's race or ethnic origin
e) information about a person's religious beliefs and criminal history
f) location information
g) copies of identity verification documents
h) biometric information, and
i) information about a person's credit worthiness, including information from credit reporting agencies.

Recommendation 2
That if recommendation 1 is not accepted, the explanatory statement explain in greater detail what types of information would fall within the scope of clause 6, why the breadth of clause 6 is justified (having regard to the associated privacy risk), and the extent to which it is intended that new CDR rules would exclude clause 6 information from the CDR.

Recommendation 3
That information about an identifiable associate is:

a) only designated to the extent that designation is justified by use cases that are outlined in the explanatory statement, and
b) subject to appropriate protections in new CDR rules, to the extent that such information may be shared pursuant to the CDR.

Recommendation 4
That the information falling within the scope of the exclusions in subclause 7(2) is excluded from the entirety of the instrument, and not just to information otherwise captured by subclause 7(1).

Recommendation 5
That draft instrument and explanatory materials clarify the scope of the location exclusion, with particular focus on highlighting that the following information is excluded from designation:

a) location information about any person (including the recipients of communications from a CDR consumer), and
b) location information of any type, regardless of the specificity of that information.

Recommendation 6
That the draft designation instrument and explanatory materials be amended to clarify the extent to which hardship and vulnerability information is designated, including in relation to:

a) the designation (or otherwise) of information about participation in government financial hardship programs and non-financial hardship or vulnerability

b) how financial hardship programs (per subclause 7(2)) differ from information about concessions or rebates (per paragraph 7(2)(e)), and
c) whether subclause 8(3) is intended to capture services or products that have been offered to a consumer on the basis that the consumer meets criteria related to disability or a need for additional assistance

and that, to the extent that hardship and vulnerability information is designated, the explanatory materials justify the designation of such information.

Recommendation 7
That consideration be given – in the designation and rule-making stages – to privacy risks associated with the inclusion of historical telecommunications information in the CDR regime, and that:

a) historical telecommunications data is only included in the CDR where there are strong use cases to support such inclusion, and
b) data holders are not required to retain data for any longer than required under the data retention scheme in the *Telecommunications (Interception and Access Act 1979)* (Cth).

Recommendation 8
That to the extent the CDR could create an alternate pathway for agencies to access telecommunications data without consumer consent and outside the TIA Act processes, the CC Act be amended to exclude that access pathway in the next package of legislative amendments to the CDR.

Recommendation 9
That the PIA at the rule-making stage explore privacy risks associated with combining data from different sectors in the CDR and any sector-specific privacy risks for telecommunications, and that CDR rules are made to mitigate these risks.

Recommendation 10
That, where practicable, the CDR rules include a common, high standard of privacy safeguards and protections for the handling of data from all sectors subject to the CDR.

Recommendation 11
That the PIA conducted at the rule-making stage assess whether the CDR could require data holders to collect, use, aggregate or store telecommunications data in new ways, and that appropriate privacy protections are implemented to address any risks arising from any such new data handling requirements.

Recommendation 12
That the PIA at the rule-making stage explore privacy risks associated with white labelling, and that CDR rules are made to mitigate these risks where applicable.

Part 1: About the OAIC and our role in the CDR system

The OAIC is Australia's independent regulator for privacy and freedom of information. The OAIC co-regulates the CDR scheme together with the ACCC. The OAIC enforces the privacy safeguards (and related CDR rules) and advises on the privacy implications of CDR rules and data standards. The OAIC is also responsible for undertaking strategic enforcement in relation to the protection of privacy and confidentiality, as well as investigating individual and small business consumer complaints regarding the handling of their CDR data.

Our goal in regulating the privacy aspects of the CDR system is to ensure that the system has a robust data protection and privacy framework, and effective accountability mechanisms to ensure consumers are protected.

Part 2: Scope of the draft instrument

Coverage of sensitive data types

The draft instrument is broad in scope and appears to capture some particularly sensitive datasets that give rise to privacy and confidentiality considerations. Much of the instrument's breadth stems from clause 6, which designates information about persons being supplied products (the customer), and their associates who use or have used those products. Such information is designated if, as per clause 6(b):

- the information was provided by the customer in connection with the supply
- the information was provided by the associate in connection with the use, or
- the information was otherwise obtained, in connection with the supply or use, by or on behalf of the entity that holds the information, or on whose behalf the information is held.

As is the case with all designated data sets, clause 6 is also subject to geographical limitations outlined in subsection 56AC(3) of the CC Act.

The question of whether clause 6 covers particular information will depend on the context in which it was collected (i.e. whether the information in question was obtained 'in connection' with the supply or use of the product). However, it would appear possible for clause 6 to include types of data I expressed concern about in my submission to the sectoral assessment consultation, including the content of communications, location data and the recipients of communications.[8] It also appears that it could include other types of sensitive information held by carriers and carriage service providers, such as such as information about a customer's race, ethnic origin, health and criminal history, identity verification documentation, religious beliefs, interests and opinions, biometric information, credit worthiness and information that is collected as a result of customer interactions with their carrier or CSP (for example, information in recorded phone conversations or available chat functions).[9] Notably, clause 6 is not subject to any exclusions or exemptions in the designation

[8] See in particular pages 4 and 5 of my submission to the sectoral assessment consultation, available at https://treasury.gov.au/consultation/c2021-198050-tc.

[9] See, for example: https://www.vodafone.com.au/about/legal/privacy; https://www.optus.com.au/about/legal/privacy; https://www.telstra.com.au/privacy#info-collect; https://www.dodo.com/sites/dodo/files/2020-09/DOD_A0800_Terms_Booklet_Privacy_Policy.pdf; https://www.foxtel.com.au/about/privacy/privacy-policy.html#q2. See

instrument itself, though I note that CDR rules may nonetheless have the effect of excluding designated data from the CDR.[10]

Many of these information types are highly sensitive. They can reveal a great deal of granular and generally confidential information about a consumer. In some cases, these datasets can also paint a detailed picture of the lives of third parties (for example, information about the recipients of communications). Depending on the data source, some of these information types may not necessarily be correct or subject to robust quality assurance processes (for example, a carrier's records of a consumer's interests or opinions may not be correct where these interests have evolved or were otherwise not confirmed by the consumer). The sensitivity of some of these datasets is further evidenced by the strict requirements already in place to limit and closely regulate the disclosure and use of relevant data.[11]

It appears that, in at least some cases, the designation of these datasets is not intended, but rather incidental to the drafting of provisions designed to capture other information types. For example, the sectoral assessment report explicitly notes an intention to exclude the substance of communications and location data from the scope of the designation instrument.[12] Furthermore, the sectoral assessment report and explanatory materials do not point to any intention to designate many of the above listed data types, and they would not otherwise appear to fall within the scope of Treasury's stated intention that the designation instrument include 'generic and publicly available product data, product data that relates to particular products used by consumers, and basic consumer and account data such as data available to consumers on their bills or through online accounts or mobile apps'.[13] In relation to data about the recipients of communications, the sectoral assessment report notes that this is intended to be captured by the designation instrument but should be excluded at the rule-making stage.[14] As noted above, the rules could also be used to exclude other sensitive, designated telecommunications datasets from the scope of the CDR.

Whilst the designation of the sensitive datasets I have identified may not be intended, there is significant risk that clause 6 nonetheless captures this information. Given the inherent sensitivity of these datatypes, I recommend that their exclusion from the scope of the draft instrument is clear on the face of the instrument and in the explanatory materials, and not be left to be excluded by the

---

also: https://www.telstra.com.au/support/mobiles-devices/switch-transfer-to-telstra; https://www.optus.com.au/for-you/support/answer?id=6551&question=how-do-i-join-optus.

[10] The sectoral assessment report notes an intention to consider excluding some datasets from the CDR via the CDR rules. See, for example, pages 24 and 31 of the sectoral assessment report, available at https://treasury.gov.au/sites/default/files/2021-11/p2021-225262.pdf.

[11] See, for example, Part IIIA of the *Privacy Act 1988* which regulates the handling of personal information about an individual's activities in relation to consumer credit; in addition, Part 13 of the *Telecommunications Act 1997* sets out strict requirements for carriers, CSPs and others in relation to their use and disclosure of personal information.

[12] See pages 22 – 23 of the sectoral assessment report, available at https://treasury.gov.au/sites/default/files/2021-11/p2021-225262.pdf.

[13] See page 3 of the sectoral assessment report, available at https://treasury.gov.au/sites/default/files/2021-11/p2021-225262.pdf. Notably, the sectoral assessment report does not identify any intention to designate web browsing history, information carriers may hold about over the top providers (though the report notes the intention to exclude over the top services as 'data holders'), information about a customer's race, ethnic origin, health, criminal history or religious beliefs, copies of identity verification documents, information about a customer's or associate's preferences, interests or opinions, biometric information or information about a person's credit worthiness.

[14] See page 24 of the sectoral assessment report, available at https://treasury.gov.au/sites/default/files/2021-11/p2021-225262.pdf.

rules. Such an approach promotes positive privacy outcomes by ensuring the exclusion of these datatypes from the CDR is clear and easily understood, thereby promoting public confidence in the CDR regime.

Should it be intended that any of the datasets listed above are to be captured by the designation instrument, justification would be required to demonstrate that their designation is reasonable, necessary and proportionate. I note that a broad designation can help to support innovative, future use cases, and additional privacy protections may be implemented at the rule-making stage (including by using the CDR rules to exclude certain data types from the CDR). However, I do not consider this sufficient justification for including more sensitive datasets within the scope of the designation instrument at this time. Rather, as outlined above, I recommend that the exclusion of these most sensitive datasets is clear on the face of the designation instrument to aid with easy comprehension and operationalisation of the CDR regime and minimise risks to personal information. Consistent with the consultation framework set out in the CC Act, I consider that any extension of the CDR to these datasets in future would warrant further consultation.

I note that clause 6 closely resembles equivalent provisions in the designation instruments for the banking[15] and energy[16] sectors. However, I do not consider that this alone justifies the inclusion of clause 6 (in its current form) in the telecommunications designation instrument. Notably, carriers and CSPs hold different and in some respects more sensitive data to banking and energy retailers – for example, the content of communications, web browsing history, and information about the recipients of communications. In this way, a broad approach to designating telecommunications data gives rise to unique privacy risks that require tailored risk mitigation strategies.

To this end, I consider that the following datasets should be clearly excluded from the designation instrument, to the extent they are held by designated data holders:

- the substance of communications
- information relating to the destination of communications – including information about the recipients of communications (unless the recipient is the CDR consumer or their associate) and web browsing history records
- data relating to 'over-the-top' services (e.g. whatsapp, social media applications, streaming services) – to the extent that this data is held by carriers and CSPs[17]
- information about a person's race or ethnic origin
- information about a person's religious beliefs and criminal history
- location information (see further information below under 'exclusions')
- copies of identity verification documents

[15] Clause 6, Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.

[16] Clause 7, Consumer Data Right (Energy Sector) Designation 2020.

[17] There is evidence that carriers and CSPs may, in some circumstances, hold some information about a customer's use of 'over the top' services– for example, when the application in question is owned on run by the carrier (see https://www.optus.com.au/about/legal/privacy#the-type-of-information-we-collect-about-you). Providers may also hold information about the use of over-the-top services where the provider bundles carriage services with other products delivered via over-the-top applications, such as television streaming or gaming products. Further, under section 187AA of the *Telecommunications (Interception and Access) Act 1979*, carriers and CSPs have data retention obligations with respect to the 'type of communication' made by a consumer. The legislation points to social media, emails and forums as examples of 'type[s] of communication' that are subject to the data retention regime – suggesting (but not confirming) that some information about a customer's use of 'over the top' services may be held by carriers and CSPs.

- biometric information, and
- information about a person's credit worthiness, including information from credit reporting agencies.

These information types could be excluded from the instrument either via an explicit exclusion, or by narrowing the instrument (and particularly clause 6) such that it is clear on the face of the instrument that these information types do not fall within the scope of designated data. The explanatory statement could then reiterate that these data types are excluded from scope.

If my recommendation to exclude the above datasets is not accepted, I recommend that the explanatory materials outline in greater detail what types of information would fall within the scope of clause 6. The explanatory materials should explain why the breadth of clause 6 is justified noting the associated privacy risk, and outline the extent to which it is intended that the CDR rules would be used to exclude information types covered by clause 6 from the scope of the CDR.

Recommendation 1
That the draft instrument be amended to clearly exclude the following information from designation, and that the exclusion of these data types be highlighted in the explanatory statement:

a) the substance of communications
b) information relating to the destination of communications – including information about the recipients of communications (unless the recipient is the CDR consumer or their associate) and web browsing history records
c) data relating to 'over-the-top' services
d) information about a person's race or ethnic origin
e) information about a person's religious beliefs and criminal history
f) location information
g) copies of identity verification documents
h) biometric information, and
i) information about a person's credit worthiness, including information from credit reporting agencies.

Recommendation 2
That if recommendation 1 is not accepted, the explanatory statement explain in greater detail what types of information would fall within the scope of clause 6, why the breadth of clause 6 is justified (having regard to the associated privacy risk), and the extent to which it is intended that new CDR rules would exclude clause 6 information from the CDR.

Information about 'associates'

Additional privacy risks emerge from the designation of information about an *associate* of a customer that relates to the associate's use of the customer's product as per clauses 6(a)(ii) and 6(b)(ii)-(iii). The sectoral assessment report and explanatory memorandum do not identify exactly what type of information would fall within the scope of these clauses. However, again, it appears possible that the information captured may reveal sensitive information about the associate including information of the type described above.

Subject to the final formulation of any telecommunications-related CDR rules, this provision appears to contemplate a situation within which data about an associate – being a person who is not directly seeking to utilise the CDR – is disclosed pursuant to the CDR. I raised a similar concern in relation to CDR in the energy sector in my submission to the consultation on the energy-related CDR rules.[18] It will be important to ensure that the designation instrument and the rules together ensure that any disclosure of data about an identifiable associate are carefully crafted so as to protect the privacy of that associate – for example, by ensuring that the associate has an opportunity to engage in the process by which their data is disclosed, and by ensuring that information about an identifiable associate is only included in the scheme to the extent that it is justified by strong use cases.

Recommendation 3
That information about an identifiable associate is:

a) only designated to the extent that designation is justified by use cases that are outlined in the explanatory statement, and
b) subject to appropriate protections in new CDR rules, to the extent that such information may be shared pursuant to the CDR.

Part 3: Exclusions

Application of existing exclusions

The draft instrument includes three explicit exclusions from the scope of designated data. Broadly speaking, these exclusions apply to:

- information that would reveal the location from which a communication was made or received, other than the location from which a call was made from a landline telephone (cl 7(2)(a), the 'location exclusion')
- information about whether a particular customer is participating in a carrier's or CSP's financial hardship program (cl 7(2)(b), the 'hardship exclusion'), and
- materially enhanced information (cl 7(2)(c), the 'materially enhanced information' exclusion).

I welcome these exclusions, which advance positive privacy outcomes by ensuring clarity in relation to the application of the CDR to particularly sensitive datasets – particularly those relating to location and hardship information.

However, there are limits of the coverage of these exclusions, which may mean that the sensitive datasets they relate to are – to some extent – 'designated' data. Notably, the exclusions only apply to information that is otherwise designated by clause 7(1) – that is, the exclusions do not apply to the broad categories of data designated elsewhere in the instrument (e.g. data designated by clauses 6 and 8). Accordingly, the information falling within the scope of the exclusions may be subject to the CDR by virtue of being captured by provisions other than clause 7(1). This appears to be at odds with the policy intention as expressed in the sectoral assessment report.[19]

[18] See Part 5, https://treasury.gov.au/sites/default/files/2021-11/c2021-200441-oaic.pdf.

[19] See pages 4 and 15 of the sectoral assessment report, available at https://treasury.gov.au/publication/p2021-225262.

In order to ensure that these sensitive information types are excluded from the designation, and consistent with recommendations 1 and 2, I recommend that the instrument is redrafted so that information that is subject to the existing exclusions are excluded from the entirety of the designation (and not just subclause 7(1)). In the event this recommendation is not adopted, the explanatory statement should justify the inclusion of these information types by reference to strong use cases.

Recommendation 4
That the information falling within the scope of the exclusions in subclause 7(2) is excluded from the entirety of the instrument, and not just to information otherwise captured by subclause 7(1).

Location exclusion

The scope of the existing location exclusion – even if applied across the entirety of the instrument – would benefit from further refinement to ensure it covers all types of location information. As currently drafted, the location exclusion relates to information 'that would reveal the location from which a communication was made or received'. The term 'communication' is not defined in the designation instrument or the explanatory memorandum. As such, it is not clear whether 'communication' is limited to contacts made between persons, or whether it would also include location data derived from a customer's use of a telecommunications product that does not involve direct communications with another person (e.g. internet usage, web browser history). Accordingly, I recommend that the location exclusion be redrafted to clearly capture any information that would reveal a person's location regardless of whether this information is linked to the making or receiving of a communication.

It appears that the existing location exclusion would cover location information about any person, and not just the relevant telecommunications account holder. For example, it appears that it would exclude location information about a third party who receives a communication from a CDR consumer. This is privacy enhancing and should be retained in any revised form of the exclusion. For clarity, I recommend that the exclusion of location information about a third party be noted in the explanatory statement.

The location exclusion also appears to exclude all types of location information – regardless of the specificity or accuracy of the data. Location information can be derived from GPS signals, Bluetooth beacons and carrier mobile towers, and the specificity of the information may depend on the source of the data.[20] However, even an approximate reference to a person's location can reveal significant insights about that person. Accordingly, I recommend that the explanatory statement clarify that the location information exclusion is intended to exclude all types of information about a person's location, regardless of the specificity of that location information.

[20] See page 28 of the sectoral assessment consultation paper, available at https://treasury.gov.au/sites/default/files/2021-08/c2021-182135-tc.pdf. See also page 12 of Telstra's submission to the sectoral assessment consultation, available at https://treasury.gov.au/sites/default/files/2021-11/c2021-198050-tc-telstra.pdf.

Recommendation 5
That draft instrument and explanatory materials clarify the scope of the location exclusion, with particular focus on highlighting that the following information is excluded from designation:

a) location information about any person (including the recipients of communications from a CDR consumer), and
b) location information of any type, regardless of the specificity of that information.

Hardship exclusion

The scope of the hardship exclusion would also benefit from further clarification (even if applied across the entirety of the instrument), particularly in regard to the following points:

- Whilst information about a customer's participation in a carrier or CSP's financial hardship program is excluded, it appears that a consumer's participation in government hardship programs could fall be within the scope of designated data. For example, the designation instrument does not exclude any record a carrier or CSP might have that a customer has a Centrelink account and receives Centrelink benefits.[21] The sectoral assessment report does not indicate whether the hardship exclusion should be limited to information about a consumer's participation in a carrier's or CSP's – but not a government's - hardship program.[22]
- It is not clear how the instrument distinguishes between 'concession or rebate' information in clause 7(1)(e) and 'hardship information'.
- It appears that the designation instrument could include non-financial hardship information – for example, information about a consumer's eligibility for priority assistance,[23] or use of a particular service for customers with disability or illness. Subclause 8(3) would appear to – on one construction – designate information indicating that a person has been offered or supplied a service for customers requiring additional assistance due to disability (as per subclause 8(2)(g)).

There are some compelling use cases for the CDR to include information about a consumer's participation in particular hardship programs, concession and rebate information, and non-financial hardship information.[24] Including these types of information in the CDR could help consumers experiencing hardship or vulnerability to secure telecommunications products and services that best serve their specific requirements. However, information about hardship and vulnerability is particularly sensitive – it can reveal, amongst other things, information about a person's health and financial situation. Given the inherent sensitivity of this type of information, the extent to which it is designated should be clear on the face of the instrument to ensure the highest possible degree of

[21] Telstra's privacy policy notes that Telstra may collect 'concession details' about a person, including a customer's Centrelink reference number – see https://www.telstra.com.au/privacy#info-collect.

[22] See for example page 23 of the sectoral assessment report, available at https://treasury.gov.au/publication/p2021-225262.

[23] Priority assistance is a level of service offered to residential consumers with a life threatening medical condition. More information is available at: https://www.tio.com.au/guidance-notes/priority-assistance-services.

[24] See pages 9-10 of the sectoral assessment report, available at https://treasury.gov.au/sites/default/files/2021-11/p2021-225262.pdf.

clarity as to the extent to which it falls within the scope of the CDR regime. To the extent that it falls within the scope of the CDR, this should be supported by strong use cases that are explained in detail in the explanatory statement.

Recommendation 6
That the draft designation instrument and explanatory statement be amended to clarify the extent to which hardship and vulnerability information is designated, including in relation to:

a) the designation (or otherwise) of information about participation in government financial hardship programs and non-financial hardship or vulnerability
b) how financial hardship programs (per subclause 7(2)) differ from information about concessions or rebates (per paragraph 7(2)(e)), and
c) whether subclause 8(3) is intended to capture services or products that have been offered to a consumer on the basis that the consumer meets criteria related to disability or a need for additional assistance.

and that, to the extent that hardship and vulnerability information is designated, the explanatory materials justify the designation of such information.

Part 4: Historical data and the earliest holding day (Clause 5)

The earliest holding day specified in clause 5 of the draft designation instrument raises privacy and confidentiality considerations with respect to the inclusion of historical telecommunications data in the CDR regime. The inclusion of historical telecommunications information in the CDR regime creates added privacy risk by increasing the scope and volume of data that can be requested and shared. Historical telecommunications data may also be less relevant and useful for consumers as it may no longer reflect the consumer's current circumstances and usage patterns. Further, historical data may be less relevant to various use cases. Accordingly, it is important that consideration is given to the extent to which historical data is included in the CDR regime and to ensuring that historical data is only included to the extent it is necessary to support use cases and accurately reflects the consumer's circumstances.

The amount of historical data that is included in the CDR regime is affected by the CC Act, the earliest holding day specified in the relevant designation instrument and the CDR rules. The draft instrument provides that 1 July 2020 is the earliest holding day for telecommunications information. This means that designated telecommunications information held by a data holder on or after 1 July 2022 will be subject to the CDR. Information obtained by a data holder before 1 July 2022 will also be subject to the CDR where it is of continuing use and relevance.[25] Additionally, the CDR rules may - and in the past have - limited the amount of historical data that providers are required to share under to the CDR.[26]

In light of the above, I recommend consideration be given – in specifying the earliest day and at the rule-making stage – to the privacy risks associated with inclusion of historical telecommunications

[25] See s 56AJ(1)(ba), CC Act.

[26] See, for example, Sch 3, cl 3.2(4)) and Sch 4, cl 3.2(6)-(7)) of the Competition and Consumer (Consumer Data Right) Rules 2020.

information in the CDR regime. Noting the sensitive nature of telecommunications data, such data should only be included where there are strong use cases to support inclusion.

The privacy risk associated with inclusion of historical telecommunications data will be further heightened if the CDR rules were to require data holders to share telecommunications data where the data would otherwise be de-identified or destroyed. Under the *Telecommunications (Interception and Access) Act 1979* (TIA Act), service providers must retain certain telecommunications data for a specified period.[27] The data retention requirements in the TIA Act are intended to ensure the availability of certain telecommunications data for law enforcement and national security purposes.[28] Service providers must comply with the *Privacy Act 1988* to the extent that their activities relate to data retained under the data retention scheme in the TIA Act.[29] This includes ensuring that personal information is de-identified or destroyed once it is no longer of use (after the mandatory retention period).[30] The draft designation instrument appears to capture a significant volume of information covered by the data retention regime in the TIA Act.[31] To reduce privacy risk, I recommend that the CDR rules do not require data holders to retain data for any longer than they are otherwise required to pursuant to the data retention scheme in the TIA Act.

Recommendation 7
That consideration be given – in the designation and rule-making stages – to privacy risks associated with the inclusion of historical telecommunications information in the CDR regime, and that:

a) historical telecommunications data is only included in the CDR where there are strong use cases to support such inclusion, and
b) data holders are not required to retain data for any longer than required under the data retention scheme in the *Telecommunications (Interception and Access Act 1979* (Cth).

Part 5: Access to designated telecommunications information as required or authorised by law

Commentary on existing telecommunications legislation articulates privacy matters that warrant consideration in the context of the designation of telecommunications information. Noting the

[27] See Part 5-1A, TIA Act.

[28] See paragraph 22, revised explanatory memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 – available at https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c/upload_pdf/501754%20Revised%20EM.pdf;fileType=application%2Fpdf.

[29] See s 187LA, TIA Act.

[30] See Australian Privacy Principle 12 as set out in clause 12 of schedule 1 to the *Privacy Act 1988*. See also Chapter 12 of the OAIC's Australian Privacy Principles Guidelines, available at https://www.oaic.gov.au/__data/assets/pdf_file/0009/1125/app-guidelines-july-2019.pdf.

[31] Relevantly, there appears to be significant overlap between the datasets captured by the draft designation instrument and the data providers must retain under the data retention scheme in Part 5-1A of the TIA Act. There also appears to be significant overlap between designated information and information protected by Part 13 of the *Telecommunications Act 1997*.

sensitive nature of telecommunications information, existing legislation creates particular protections for how this information must be handled. This includes limits on how that information can be disclosed, and how it can be accessed by government agencies.[32] The draft designation instrument appears to capture a significant volume of information protected by existing regulatory regimes, most relevantly the TIA Act and *Telecommunications Act 1997* (Telecommunications Act).[33]

Subject to the making of the designation instrument and any subsequent CDR rules, there is risk that s 56EI(1)I of the CC Act could allow for the disclosure of telecommunications data outside the scope of the protections in the TIA Act and without consumer consent. Section 56EI(1)(c) of the CC Act allows an ADR to use or disclose CDR data without the consumer's consent where the use or disclosure is 'required or authorised by' or under another Australian law or an order of a court or tribunal. The Parliamentary Joint Committee on Intelligence and Security (PJCIS) has observed that a similar 'required or authorised by' law exception in the Telecommunications Act has been used by some agencies to access telecommunications data.[34] If s 56EI(1)(c) was used by agencies in a similar way, this would have the practical impact of reducing the effectiveness of safeguards in the TIA Act that exist to mitigate the privacy effect of allowing access to telecommunications data.

In order for an agency to use s 56EI(1)(c) of the CC Act to collect consumer data from an ADR, the agency would need to be aware that the ADR held the relevant data. Whether the ADR holds relevant information may not always be clear, and agencies may therefore find it easier to access telecommunications data under different access pathways (most relevantly, directly from a carrier or CSP). On this basis, in practice it would appear generally unlikely that s 56EI(1)(c) would be used as an alternate pathway to access telecommunications data.

That said, any unintended access pathways to telecommunications information should be addressed. This is particularly important in relation to s 56EI(1)(c) because ADRs may have limited experience in navigating the telecommunications regulatory landscape and may find it difficult to assess whether the disclosure of information to an agency is required or authorised by law. Accordingly, while it may be considered a low risk, I recommend that to the extent the CDR could create an alternate pathway for agencies to access telecommunications data without consumer consent and outside the processes in the TIA Act that in due course the CC Act be amended to exclude that access pathway.

[32] See the access limits in the TIA Act. See also the protections for telecommunications information in Part 13 of the *Telecommunications Act 1997*.

[33] Relevantly, as noted above there appears to be significant overlap between the datasets captured by the draft designation instrument and the data providers must retain under the data retention scheme in Part 5-1A of the TIA Act. There also appears to be significant overlap between designated information and information protected by Part 13 of the *Telecommunications Act 1997*.

[34] For further information, see Part 3 of the Parliamentary Joint Committee on Intelligence and Security's 2020 review of the mandatory data retention regime report – available at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime/Report.

Recommendation 8
That to the extent the CDR could create an alternate pathway for agencies to access telecommunications data without consumer consent and outside the TIA Act processes, the CC Act be amended to exclude that access pathway in the next package of legislative amendments to the CDR.

Part 6: Cross-sectoral privacy and confidentiality considerations

Combining data from various sectors means richer and more granular insights may be derived about individual CDR consumers, while this can have benefits for consumer, it also increases the overall privacy risks for consumers participating in the CDR.[35]

The PIA conducted by Treasury and attached to the final sectoral assessment consultation considered the cumulative privacy and security risk associated with combining datasets from multiple sectors.[36] The assessment noted that the CDR is intended to be an economy-wide framework and referenced existing privacy and consumer protections in the CDR scheme as mitigating the risk associated with combining cross-sectoral CDR data.[37] I agree that existing privacy, confidentiality and security requirements in the existing CDR Rules (the *Competition and Consumer (Consumer Data Right) Rules 2020*) and data standards create a strong foundation to protect consumers' information as the CDR continues to grow. I consider further analysis regarding cross-sectoral privacy and confidentiality considerations would be valuable at the rule-making stage in two respects.

First, thorough analysis should occur when telecommunications-related CDR rules are made to ensure that the CDR operates as intended and any privacy risks arising from combining cross-sectoral data in new ways are adequately addressed. I recommend that further analysis is conducted in the PIA at the rule-making stage to assess the impact of combining telecommunications information covered by the designation instrument with banking and energy data already covered by the CDR. This should include understanding new information flows and data sets, and associated privacy and confidentiality risks.

Second, it is important that a common high standard of privacy protections exists between designated sectors to the extent that this is practicable. Currently, the *Competition and Consumer (Consumer Data Right) Rules 2020* include general privacy protections applicable to all designated sectors, as well as schedules containing specific rules for the banking and energy sectors. Where practicable, it is desirable that privacy protections are standardised across sectors. This approach helps to ensure that consumers are generally afforded the same privacy protections regardless of the particular datatypes that are relevant to their CDR needs. Setting a common standard of protections

[35] See page 5 of my submission to the telecommunications sectoral assessment consultation process – available at https://treasury.gov.au/consultation/c2021-198050-tc.

[36] See page 40 of the sectoral assessment report, available at https://treasury.gov.au/sites/default/files/2021-11/p2021-225262.pdf.

[37] See page 40 of the sectoral assessment report, available at https://treasury.gov.au/sites/default/files/2021-11/p2021-225262.pdf.

(where practicable) also helps to ensure that the CDR is easily understood by participants and consumers and reduce the risk of error in the application of privacy safeguards to datasets across sectors.

That being said, I also accept that some differences in the application of CDR rules between sectors may be required in order to appropriately address sector-specific privacy risks. As such, I further recommend that the PIA at the rule-making stage identify and assess sector-specific privacy risks for the telecommunications sector, and advise on whether any sector-specific CDR rules are required to mitigate these risks.

Recommendation 9
That the PIA at the rule-making stage explore privacy risks associated with combining data from different sectors in the CDR and any sector-specific privacy risks for telecommunications, and that CDR rules are made to mitigate these risks.

Recommendation 10
That, where practicable, the CDR rules include a common, high standard of privacy safeguards and protections for the handling of data from all sectors subject to the CDR.

Part 7: Other issues

Designation of billing and account information about retail supplies of products (clause 7)

I am aware of stakeholder consideration of whether clause 7 of the draft instrument could, subject to relevant CDR rules, require carriers and CSPs to collect or collate information in new ways. It is important that any new data flows arising from the designation instrument and related CDR rules are appropriately considered. To the extent practicable, provider obligations should be clear in the designation, CDR rules and explanatory materials, to reduce the risk of data being collected, aggregated or stored in ways that are not required or anticipated by the CDR scheme.

Clause 7 designates certain billing and account information about retail supplies of products as CDR data. The explanatory statement indicates clause 7 is intended to cover information customers typically have access to on a bill or general account information, which might be accessible online or via a mobile application.[38] Notwithstanding the intention to capture information already available to consumers, the explanatory statement notes that the information in section 7 is designated regardless of whether the information appears on every customer's bill.[39]

I consider the risk that the CDR will result in providers collecting new information is low, having regard to relevant provisions in the CC Act and the overlap between information in the draft

[38] See page 5 of the exposure draft explanatory materials, available at https://treasury.gov.au/sites/default/files/2021-11/c2021-224994-explanatorymaterials.pdf.

[39] See page 5 of the exposure draft explanatory materials, available at https://treasury.gov.au/sites/default/files/2021-11/c2021-224994-explanatorymaterials.pdf.

designation instrument and information covered by the data retention scheme in the TIA Act.[40] That said, I consider that participants should be provided with clear advice on this point (whether it be through the CDR rules, public guidance, or other explanatory materials). I also consider there is a risk that providers may be required to store or aggregate data in new ways to comply with their CDR obligations.

To best protect privacy and confidentiality, I recommend that the PIA conducted at the rule-making stage consider current arrangements for the collection, use and storage of designated data sets, and assess whether the CDR could require providers to handle telecommunications data, including clause 7 data, in new ways. If the CDR could result in carriers and CSPs collecting, storing or aggregating telecommunications data in different ways, appropriate privacy protections should be considered and implemented in the CDR rules. The CDR rules, and accompanying explanatory materials, should also clarify provider obligations regarding new data flows, to reduce the risk of data being handled in ways that are not required or anticipated by the CDR scheme.

Recommendation 11
That the PIA conducted at the rule-making stage assess whether the CDR could require data holders to collect, use, aggregate or store telecommunications data in new ways, and that appropriate privacy protections are implemented to address any risks arising from any such new data handling requirements.

White labelling arrangements

The explanatory statement indicates that the designation instrument is intended to capture white labelled products.[41] This is consistent with existing arrangements within which white label products are included in the CDR.[42] White label products are typically created and operated by one entity (a white labeller) and branded and retailed to consumers by another entity (a brand owner). White labelling is common in industries including banking and telecommunications. An example of white labelling in the telecommunications sector is where a carrier (the white labeller) provides core telecommunications products (e.g. broadband, voice or mobile services) and support services (e.g. onboarding or payments), and a brand owner markets the product and handles sales and customer relationships.

As a general comment, white labelling arrangements can give rise to unique privacy risks in a CDR context. Consumer consent is the bedrock of the CDR regime and a key mechanism through which consumer privacy and confidentiality is protected. Privacy and confidentiality is best protected where consent is informed and specific. Because white labelling involves multiple businesses providing a single product to a consumer, there is a risk it may not always be clear to the consumer who in the

[40] In the CC Act, see the definition of data holder in s 56AJ and the power to make consumer data rules in Part IVD, Division 2, Subdivision A. In the TIA Act, see Part 5-1A.

[41] See page 4 of the exposure draft explanatory materials, available at https://treasury.gov.au/sites/default/files/2021-11/c2021-224994-explanatorymaterials.pdf.

[42] See Australian Government guidance titled 'Approach to disclosure of consumer data: white label products', available at https://www.cdr.gov.au/sites/default/files/2020-12/CDR%20-%20Guidance%20on%20white%20label%20products%20-%2022%20December%202020.pdf.

white labelling arrangement is the relevant CDR participant (i.e. whether it is the white labeller or the brand owner), and which entity will receive and use data pursuant to the consumer's consent. This has the potential to undermine informed and specific consent.

White labelling arrangements can vary between sectors and therefore give rise to sector-specific (in addition to more general) privacy risks in the CDR context. As such, I recommend that the PIA at the rule-making stage explore privacy risks associated with the CDR coverage of white labelled telecommunications products, and that CDR rules are made to mitigate these risks.

Recommendation 12
That the PIA at the rule-making stage explore privacy risks associated with white labelling, and that CDR rules are made to mitigate these risks where applicable.