Australian Government
The Treasury

Consumer Data Right

Consumer data right: Telecommunications sectoral assessment

Final report

November 2021

Manager
Media and Speeches Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

Contents

Glossary

ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
Act	*Competition and Consumer Act 2010* (Cth)
ADR	An accredited data recipient is a person accredited by the ACCC to receive CDR data with a consumer's consent
API	An application programming interface is software designed to help other software interact with an underlying system
Carriage service provider (provider)	A carriage service provider has the same meaning as in the Telecommunications Act. A carriage service provider supplies a carriage service to the public using a network unit owned by one or more carriers
Carrier	A holder of a carrier licence granted under the Telecommunications Act
CDR	The Consumer Data Right is a right for Australian consumers – individuals and businesses – to access data held about them, and the regime that facilitates such access
CDR consumer	The term 'CDR consumer' is defined at section 56AI(3) of the Act and includes natural persons and businesses. An eligible CDR consumer can give consent to an accredited person to collect their CDR data from a data holder
CDR rules (rules)	*Competition and Consumer (Consumer Data Right) Rules 2020*
Data holder	The term 'data holder' is defined in section 56AJ of the Act and includes persons specified in a designation instrument (section 56AJ(2))
Designation	Designation refers to the designation of a sector to be subject to the CDR by reference to datasets and data holders in a designation instrument, as defined below
Designation instrument	A legislative instrument made by the Minister under section 56AC of the Act
NBN	National Broadband Network
OAIC	Office of the Australian Information Commissioner
Standard/s	The data standards made by the Data Standards Chair under section 56FA of the Act
Statutory factors	The factors that must be considered by the Minister under section 56AD(1) of the Act before making a decision to designate a sector
Telecommunications Act	*Telecommunications Act 1997* (Cth)
Telecommunications Consumer Protection Code	Industry code which is registered under section 136 of the Telecommunications Act

1. Executive Summary

In November 2017, the Australian Government announced the introduction of the Consumer Data Right (CDR), with application initially in the banking, energy and telecommunications sectors. In May 2021, the Prime Minister, the Treasurer, and the Minister for Superannuation, Financial Services and the Digital Economy announced that Treasury would conduct a sectoral assessment to consider whether to extend the CDR to the telecommunications sector. Expanding the application of the CDR is a key initiative in the government's Digital Economy Strategy, announced in the 2021-22 Budget.

Designating a sector is a threshold decision for applying the CDR to data within a sector. Designation involves specifying classes of information (data) as well as the data holders that could ultimately be required to share CDR data under the CDR rules. The sectoral assessment process is a necessary precursor to the Minister deciding whether to designate a sector, and in what form.

Following the government's announcement in May 2021, Treasury has consulted on a telecommunications designation. As part of our assessment, we invited submissions on a consultation paper, conducted bilateral meetings and held stakeholder roundtables. We also undertook a targeted round of stakeholder consultation to assess regulatory cost impact, assisted by Grant Thornton. Drawing on this input, we evaluated the impact of designating the sector by reference to a range of factors including consumer benefit, public benefit and regulatory impact.

There are a range of benefits to consumers – both individual and business users – and the public interest from designation. The CDR enables Accredited Data Recipients (ADRs) to provide information and services to individuals and businesses. ADRs could use information provided by the CDR to find the most suitable product for consumers in a timely manner, better monitor usage, and facilitate engagement in the telecommunications market, thereby improving market efficiency. This may be of particular benefit to small business consumers, who often lack time to engage meaningfully in the market, and vulnerable consumers, who may face barriers to such engagement. As the third CDR sector, designating the telecommunications sector will also promote cross-sectoral innovation and access to the digital economy.

Balancing this, stakeholders raised issues regarding the potential regulatory impacts and noted the scope of the designation was important for assessing such impacts. Support for designation from existing data holders was in many cases contingent on minimising the costs of any new obligations to hold or store data, and that any implementation of the CDR has regard to the overall infrastructure build that would be necessary to support data sharing.

Treasury's recommendation is that the telecommunications sector be designated for the CDR. This recommendation is made after consideration of the range of statutory factors required to be assessed in a sectoral assessment and the feedback received during consultation.

We consider it is appropriate that the designation support data sharing similar to that in the banking and energy sectors. As a result, we recommend a designation that includes 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. The entities that hold this information and could therefore be required to share this information as data holders, are retail service providers in the telecommunications sector.

Treasury considers that the issues raised during consultation regarding privacy and regulatory impact can be managed by this proposed designation scope and the ability to further manage

impacts at the rule- and standards-making stage. At these stages, consultation will inform design and implementation decisions including the precise datasets to be shared, phased commencement of data sharing obligations, and the extent to which mandatory obligations should apply to all providers in the sector or select providers.

There are several datasets explored during consultation which we do not consider appropriate for designation at this time. These include coverage map data, the content or substance of communications, location or phone cell tower data, broadband speed data, and information about hardship arrangements. While we do not think designation is appropriate at this time, there is potential for these datasets to be reconsidered for designation in the future, subject to further assessment and consultation. With the exclusion of broadband speed data, network providers (such as NBN Co) would not be a data holder under the proposed designation.

2. Designating a sector under the CDR regime

2.1 The Consumer Data Right

The CDR was conceived as a right by the Productivity Commission in 2017. The Commission identified an expectation on the part of consumers to have greater access to the data collected about them.[1] The finding was based on the potential benefits to individuals and businesses from increased awareness of, and access to, their own consumer data.

The CDR is a significant economy-wide reform designed to empower consumers to benefit from the data Australian businesses hold about them and, in doing so, strengthen competition, innovation and productivity in designated sectors. The CDR has been designed to apply to the whole Australian economy and is being activated sector-by-sector, based on datasets and sectors of greatest consumer value.

The CDR gives consumers a right to consent to data held about them being shared with accredited and trusted third parties, to help consumers derive direct benefits from that data. The CDR can help consumers navigate important decisions and milestones in their lives and facilitate access to better value and more personalised products and services within and across sectors.

2.2 The CDR sectoral designation process

The Minister may designate a sector of the Australian economy to be subject to the CDR under section 56AC of the *Competition and Consumer Act 2010* (the Act). A sector is designated by legislative instrument, which specifies the classes of information (or data) designated for the purposes of the CDR and the class or classes of persons who hold the designated information (data holders). The Act provides that before a sector can be designated, certain matters under section 56AD(1) (collectively, the statutory factors) must be considered by the Minister. These include:

- the interests of consumers;
- promoting competition;
- the efficiency of relevant markets;
- promoting data-driven innovation;

[1] Productivity Commission, 2017. *Data Availability and Use* Inquiry Report, pp. 83-85.

- the privacy or confidentiality of consumers' information;
- any intellectual property in the information;
- the public interest; and
- the likely regulatory impact of designation.

The Act also requires that before designating a sector, the Minister must be satisfied that the Secretary of the Department (the Treasury) has arranged for consultation and analysis about designation and published a report about that analysis and consultation. As part of its consultation, the Treasury is required to consult the Australian Competition and Consumer Commission (ACCC), Office of the Australian Information Commissioner (OAIC), and the primary regulator of the relevant sector (section 56AE(1)(c)). The making of a designation instrument cannot occur until 60 days after the publication of the report. Before making a designation instrument, the Minister must also consult the OAIC about the likely effect of the instrument on the privacy and confidentiality of consumers' information (section 56AD(3)).

2.3 Effect of designation

The making of a designation instrument enlivens the rule-making power in relation to the sector by specifying the parameters for the classes of information that the rules may require to be shared under the CDR in a particular sector, as well as who is required to share it as a designated data holder. Once a sector has been designated, CDR rules and standards for that sector can be made in accordance with statutory processes, including extensive consultation requirements.

Designation involves specifying 'classes of information' or data to be designated, but designation of a sector does not itself impose substantive obligations. The requirement to disclose particular data arises from the CDR rules, which establish what is 'required' CDR data that must be shared in response to a valid request, as well as what information data holders are 'authorised' to share on a voluntary basis. The rules may do this with more specificity than the designation instrument. In turn, the data standards specify the technical fields and formats that data is ultimately shared in.

The rules have been developed to apply universally across sectors to the extent possible, however, sector-specific provisions and modifications are catered for in sector-specific schedules. Once designation of a sector occurs, sector-specific issues (for example, external dispute resolution arrangements specific to that sector) are considered, as well as the development of sector-specific data standards.

3. Telecommunications sectoral assessment

3.1 Consultation

On 22 July 2021, the Treasury published a consultation paper as part of the telecommunications sectoral assessment seeking views about the proposed designation of the telecommunications sector by reference to the statutory factors including the likely regulatory impacts of designating the sector.

Consultation closed on 19 August 2021 and 18 submissions were received. Treasury held meetings with industry stakeholders, consumer groups and government departments, including in relation to the potential regulatory impact of designation.

In addition, in July 2021 Treasury consulted on a Strategic Assessment to inform the government's roadmap for the economy-wide rollout of the CDR. Submissions received in relation to that process have also been considered in preparing this report where relevant to the potential designation of telecommunications, including with respect to cross-sector benefits of designation.

3.2 Overview of stakeholder views

Submissions were received from a range of stakeholders with different perspectives on the potential designation of the telecommunications sector. Many existing sector participants and industry bodies raised concerns about designation and questioned the extent of potential benefits. Privacy issues were raised by some stakeholders, particularly about the designation of certain datasets, such as location data and metadata.

Feedback in support of designation, including the potential for a telecommunications designation to facilitate cross-sector use cases, was received through submissions as well as through the Strategic Assessment consultation process and during bilateral meetings. A number of submissions from providers indicated in-principle support for designation and considered the key question to be the scope of designation, highlighting issues relating to more complex datasets. The ACCC and the Australian Communications and Media Authority (ACMA), and consumer advocate Australian Communications Consumer Action Network (ACCAN), provided submissions in support of designation, noting the role that the CDR could play to reduce information asymmetries and assist consumers in making decisions about services that best suit their needs. The OAIC also provided a submission which considered matters relevant to the privacy or confidentiality of consumers' information and included detail about privacy impacts arising from the possible designation of certain sensitive datasets, including (but not limited to) location data and metadata. The potential regulatory impact of designating the telecommunications sector was raised at a high level in submissions, with a particular focus on the potential impact on smaller participants who may face a greater cost of compliance, relative to larger participants. Further information on this issue was provided as part of industry engagement on regulatory impact, discussed below.

4. Analysis of statutory factors

4.1 The interests of consumers

We consider there would be benefits to consumers from designating the telecommunications sector. Designation could support ADRs to innovate and design products and services that promote convenience for consumers, particularly on a cross-sector basis. For example, the CDR could enable

ADRs to provide consumers with a holistic picture of their financial position and their use of essential services in one place.[2] Consultation also raised use cases that could be supported with telecommunications data alone, such as use cases that support switching and product comparison.

The CDR can help consumers find products that best meet their needs

Designating the telecommunications sector, and in particular, designating product data and consumer data that show how consumers use existing telecommunications services, could make it easier to make better decisions when selecting a service.

Currently, comparing telecommunications services can be a complex exercise for consumers. As ACCAN notes:

> the wide range of complex and competing products and services in the telecommunications sector can put consumers at a disadvantage when identifying and selecting appropriate services.[3]

The ACCC and the ACMA consider the complexity of price and non-price elements of telecommunication services makes it hard for consumers to compare 'like-for-like' and make meaningful assessments of their options. The ACMA suggests this accounts, at least partially, for relatively low levels of switching in the sector.[4] However, some stakeholders believe complexity has decreased in recent years with a shift to unlimited data for most fixed-line plans and the inclusion of unlimited calls and texts in most mobile phone plans.[5]

Designating the telecommunications sector has the potential to deliver consumer benefits by facilitating access to, and improving the use of, information about telecommunications services and how consumers use them.[6] This could empower consumers to make more informed decisions and secure better products. The CDR can make it easier to compare products and services by standardising the expression of their features for the purpose of sharing product data.[7] To best support this, generic product data would need to be designated as well as data that shows how consumers use telecommunications products (such as usage data), so ADRs can match consumers' needs to products.

Stakeholders noted that existing regulatory and industry code disclosure obligations require providers to make product information available to consumers.[8] Requirements such as providing consumers with Critical Information Summaries and Key Facts Sheets are intended to help them make informed purchasing decisions and more easily compare products and services.[9]

In our view, designating generic telecommunications product data can build on and enhance the effectiveness of these initiatives. These documents are not required to be provided in a standardised or machine-readable format under existing regulation and need to be reviewed separately by consumers to compare them, which can be time consuming. Collecting the information in these disclosure documents under the CDR in a standardised, machine-readable format, and allowing

[2] AGL Energy submission, p. 1.
[3] ACCAN submission, p. 3.
[4] Ibid, p.4; ACMA submission, p. 4.
[5] Telstra submission, p.7; Communication Alliance submission, p. 10.
[6] ACCC submission, p. 4.
[7] ACMA submission, p. 4.
[8] Optus submission, p. 8; Comms Alliance submission, p. 10; Telstra submission, p. 10.
[9] ACMA submission, p. 6.

consumers to share consumer data that shows how they use telecommunications services with ADRs, could dramatically improve the usability of this data for comparison and consideration of the plans or products that will best meet a consumer's needs.[10] The CDR may also promote competition by enabling services offered by smaller providers to be more easily identified and considered by customers.

While comparison websites and usage calculators already provide estimates and product recommendations, these tools rely on consumers manually inputting information about their usage and evaluating the best deal themselves. ADRs that provide tailored product recommendations can relieve consumers of manual input and:

> improve consumers' ability to exercise informed choice by effectively allowing a consumer to outsource the burden of understanding their own personal usage patterns and analysing these to select a service suited to their needs.[11]

ADRs could also combine usage data from different telecommunications services (for example, mobile and broadband) and from multiple providers to present a holistic picture of how a consumer uses telecommunications.

More convenient data-driven services can help consumers spend less time on 'life admin' and reduce transaction costs. The CDR has the potential to support consumers to plan for and better manage significant financial events, such as moving house or setting up a new business. As more sectors are designated to the CDR, consumers will be able to more easily compare bundles that combine products and services from multiple sectors.[12]

Some stakeholders consider usage data of limited use to consumers given the market trend towards unlimited calls, SMS and data on most plans.[13] While this is the case for many NBN fixed line and wireless plans, data limits remain a feature of a significant proportion of mobile, mobile broadband and NBN satellite plans. Limited plans that allow customers to pay for the usage they need will continue to be favoured by certain customer segments, such as low-income customers or individuals with limited data needs.

Consumers can consent to their data being collected on a 'one time' or ongoing basis under the CDR rules. Ongoing services could allow ADRs to perform a monitoring function for consumers. If an ADR checks a consumer's usage patterns against offers on the market occasionally (for example, once a week or month), it could notify the consumer when their needs and market offers have diverged and they should consider changing to a better offer.

Service quality and performance data

The consultation paper noted service quality and performance data as non-price factors that are of interest to consumers yet difficult to compare. Examples of service quality or performance data may include call centre response times, complaints data regarding service delivery, or the time it takes to install a connection.[14] In its submission, the ACMA notes that non-price factors are ranked highly by consumers in the aspects of telecommunications services that are most important to them.[15]

---

[10] Ibid, p. 6.
[11] Ibid, p. 4.
[12] AGL submission, p. 6.
[13] Telstra submission, p. 9; Communication Alliance submission, p. 10.
[14] A comprehensive list of service quality data is included in ACMA's submission, p. 3.
[15] ACMA submission, p. 3.

Submissions also noted a general lack of specific and standardised data, and consistent definitions, for measuring and comparing service quality and performance data across the industry.[16] Some high-level and aggregate statistics on complaints in the sector are publicly available through the Telecommunications Industry Ombudsman[17] and the ACMA,[18] however, the CDR can only require product data about performance to be shared to the extent it is made publicly available by data holders.[19]

The proposed scope of designation includes product information that may cover, at the rule-making stage, service quality or performance data relating to a particular product and is publicly available.[20] However, there are no datasets the CDR rules could capture that could support the type of meaningful product comparison that was identified as useful in the consultation process. Information such as the number of complaints per product is not publicly available and could therefore not currently be mandated for data sharing under the CDR rules. It should be considered whether, over time, the rules require information of this kind to be shared if publicly available and published in a standardised and easily comparable way. If so, such requirements would be subject to further consultation and consideration of regulatory impacts.

Broadband speed data

Consumers have access to different broadband technology based on their location, and when the supply reaches residential premises. Wholesale connectivity is usually provided by the NBN. Data relating to the transmission speeds can be captured by both network providers like NBN Co, and retailers providing services over these networks. Some submissions noted the potential consumer benefit in designating broadband speed data, particularly for product comparison.[21]

Data about speed performance over the NBN network is recorded by NBN Co throughout the day and made available to retailers.[22] However, several submissions noted that actual speeds observed by a customer are affected by various factors beyond the layer provided by NBN Co.[23] Therefore, to provide a comprehensive picture of a customer's actual broadband speeds, any data relating to an individual consumer or premises provided by NBN Co would need to be augmented by data held by that customer's retailer relating to performance at the premises.

Concerns were raised during consultation on the potential designation of data collected by retailers regarding the speeds available to their customers. The broadband speeds a consumer experiences can be attributed to a range of factors relating to the supply chain and factors beyond the influence of retailers (for example, surrounding infrastructure and wiring or weather events), making this information difficult to usefully compare even with both wholesaler and retailer speed data. Sharing this information could, therefore, have unintended consequences; for example, if deviations from expected speeds are interpreted as being caused solely by the retailer. The utility of the information for product comparison is also diminished when considering that the range of factors that ultimately influence speeds mean that past performance is not an indication of speeds that could be obtained in the future. Further, the way this data is collected now is not standardised to a sufficient degree.

[16] Communications Alliance submission, p. 15.
[17] Telecommunications Industry Ombudsman Annual Report 2020-21, p. 44, p. 78.
[18] ACMA submission, pp. 6-7.
[19] Section 56BF(1) of the Act.
[20] Ibid.
[21] ACCC submission, p. 5; ACCAN submission, p. 6.
[22] NBN Co submission, p. 7.
[23] Ibid, p.4; Telstra submission, p.11; Communications Alliance submission, p. 14.

While we see potential benefits related to some broadband speed data, we do not consider that existing broadband speed data could support meaningful service comparison and recommend that this dataset be revisited at a later stage.

Submissions also noted the existing information available to consumers regarding broadband speed performance.[24] Broadband providers are required to provide consumers with information about the typical speed of each of their NBN broadband plans in the busy evening period (7–11 pm) and some information regarding their maximum line speed if advertised off peak speeds are not achieved.[25]

Network coverage data

Consumers can currently access coverage maps from the websites of the 3 mobile network operators (Telstra, Optus, and TPG) to determine coverage in their area. Australia-wide telecommunications infrastructure data is also available in map form[26], or via publicly available application programming interfaces (APIs) [27].

The potential for coverage data to support consumers when deciding between retailers was noted in the consultation paper. However, several submissions noted the accuracy of coverage maps can be limited due to external factors such as topography and the physical qualities of nearby structures.[28] Furthermore, the data used to develop coverage maps is not currently measured in a standardised way. Therefore, we do not consider that designating the information that underlies coverage maps would achieve the desired outcome of supporting consumers in making decisions based on meaningful coverage comparison at this time.

The CDR can support vulnerable consumers' market participation

At its broadest, consumer vulnerability refers to:

> circumstances that cause difficulty in using markets or in receiving adequate products and services; or which heighten the risk of harm, detriment, or disadvantage to consumers.[29]

Age, location, English language proficiency, financial situation, health, and presence of permanent or temporary disability are some of the factors affecting consumers' vulnerability.[30] Some consumers have special needs due to temporary, situational or ongoing vulnerability relevant to the supply of telecommunications services.[31] The interests of vulnerable consumers are critical in considering the impact of designation on consumers.

Designating information about accessibility features or services for customers with a disability or life-threatening condition could make it easier for vulnerable consumers to identify and compare products that support specific needs.[32] Designating billing data, including information about

---

[24] NBN Co submission, p. 5; Communications Alliance submission, p. 10.
[25] Australian Competition and Consumer Commission, 'Broadband speeds', accessed at: https://www.accc.gov.au/consumers/internet-landline-services/broadband-speeds
[26] Radio Frequency National Site Archive, accessed 14 September 2021 at: https://www.rfnsa.com.au/?first=1
[27] https://www.acma.gov.au/radiocomms-licence-data
[28] Communications Alliance submission, p. 15; Telstra submission, p. 8.
[29] Consumer Policy Research Centre, 2021, *Vulnerability, capability and opportunity, understanding consumer vulnerability as a key to unlocking benefit from the Consumer Data Right*, available from: Consumer Data Right ...~https://cprc.org.au/publications/consumer-data-right-report-3-vulnerability-capability-opportunity-understanding-consumer-vulnerability-as-a-key-to-unlocking-benefit-from-the-consumer-data-right/
[30] ACCC submission, p. 8.
[31] Ibid, p. 6.
[32] ACCC submission, p .5.

government concessions or rebates, may assist vulnerable consumers to find more competitive service offerings. For example, if a consumer is on a government concession and this is disclosed as part of a consumer data request for product comparisons, other providers may adjust their pricing structure to reflect similar concessions within their business. The ACMA considers the use of consumer data to assess sources of debt for those in financial hardship and determine better ways to manage that debt a valuable use case of the CDR.[33]

The benefits of such tailored product comparisons could be helpful for consumers in financial distress or on low incomes by identifying services they are paying for but not using (for example, paying for usage they do not need).

The CDR can help small businesses to find products that best meet their needs

Small businesses have varying telecommunications needs, but they are typically more complex than residential customers.[34] Small businesses may use comparison websites to find the best deal, but often struggle to find bespoke offerings. Searching for a telecommunications deal is not usually a priority for many small businesses that want to save time and have the process simplified.[35] ADRs that match business needs to commercial offerings are likely to be of significant value to small business consumers with limited resources and high service continuity requirements.[36] Consultation also revealed that billing data sets could be useful for ADRs to facilitate business administration or management services for small businesses.

4.2 Promoting competition and market efficiency

The CDR aims to facilitate and promote greater competition in designated sectors to improve efficiency for consumers. Telecommunications was explored by the Productivity Commission as a sector that collected data on users and that consumers in the sector may be able to use that data to solicit competitive offers from other providers.[37] By enabling ADRs to assist consumers to navigate market complexity and make better decisions, the CDR aims to encourage greater efficiency in the telecommunications market and boost the level and nature of competition in the market.

A range of perspectives were presented in submissions about the CDR's potential to increase efficiency in the telecommunications market.

ACCAN noted the potential for the CDR to reduce information asymmetries between consumers and providers and therefore reduce barriers to switching[38] and increase consumer surplus[39]. It suggested this can be done through comparators that can make individualised recommendations.[40] The ACCC noted the complexity and product differentiation in the market, with hundreds of offerings in the market constituting a 'wide range of complex and competing products and services'.[41] The ACCC

[33] ACMA submission, p. 5.
[34] Australian Small Business and Family Enterprise Ombudsman submission, p. 1.
[35] The Office of Communications (UK) 2020, *Open Communications: Research Findings,* available from: Open Communications qualitative research (ofcom.org.uk)
[36] ACMA submission, p. 4.
[37] Ibid, pp. 81-84.
[38] ACCAN submission, p. 8
[39] Ibid, p. 9.
[40] Ibid, p. 8.
[41] Ibid, p. 3.

considers there are 'high information asymmetries between service providers and consumers', which complicates consumer decisions and increases the risk of inefficient purchasing decisions.[42]

The ACCC noted the CDR could play a role in improving the nature of competition in telecommunications markets:

> Greater transparency promotes competition by facilitating informed consumer participation in the sector, and incentivising market participants to compete on the merits of their products and services rather than adopting opaque and confusing marketing strategies.[43]

The ACCC also noted the role the CDR could play to assist consumers navigating the combination of technically complex products and retail offers:

> Technically complex products and complex retail offers can obscure the benefits and limitations of services in a multiplicity of bundles, temporary promotions and discounts, a telco CDR would support consumers to penetrate this complexity.[44]

Submissions indicated that existing disclosure documents are intended to assist consumers to compare retail offers in the telecommunications markets. Optus noted that consumers are generally satisfied with the information they receive in their interactions with telecommunications providers, whether on a bill or at the point of sale.[45] Some of these disclosures are the product of regulatory requirements to disclose information, such as Critical Information Summaries and Key Facts Sheets. The Communications Alliance noted that Critical Information Summaries 'are well received by customers and provide an important role in customers' purchasing decisions'.[46] While these regulations are important for improving information disclosure in the sector, issues remain. The ACMA noted a risk of 'information overload' where more information does not necessarily equate to better choices.[47] The documents are not required to be standardised and can lead to time consuming product comparisons. Machine readability could 'dramatically improve the usability of the data'.[48] The CDR can make a difference by making already-available information more easily utilised through machine readability.

Designation will enable consumers to make well-informed decisions and therefore promote efficiency and competition in the telecommunications market. The CDR will allow consumers to use an ADR to match their needs to products and retail offers in the telecommunications market. An ADR will be able to analyse a consumer's data, compare their needs to market offerings and recommend telecommunications solutions tailored to their requirements and budget. ADRs with monitoring and alerting services will assist consumers with changing needs to respond to changes to products and services offered by telecommunications companies. In this way, the CDR can help consumers gain greater value from their telecommunications service and enhance demand-driven competition in the sector.

[42] ACCC submission, p. 9.
[43] Ibid, p. 10.
[44] Ibid, p. 10.
[45] Optus submission, p. 9.
[46] Communications Alliance submission, p. 10.
[47] ACMA submission, p. 6.
[48] ACMA submission, p. 6.

4.3 Promoting data-driven innovation

Access to greater volumes of standardised consumer and product data will support innovation and create new business opportunities for third parties seeking to use the data to offer new or improved services to consumers. Opportunities will be generated for existing service providers to expand or improve their offerings as more data is shared across more sectors. As stated by AGL:

> the longer-term benefit of CDR is the ability for service providers to innovate across the various CDR designated sectors and provide consumers with holistic multi-services in a convenient one-stop shop arrangement.[49]

Providing product information in a standardised digital format will enable more efficient comparison and give smaller participants or new entrants an opportunity to make consumers aware of their products. As the ACCC noted:

> smaller players, who can adapt to changing market circumstances more quickly than larger players, may release tailored, new, or niche products in response to new information about consumers' needs and to compete with other services in the market.[50]

If the data can reveal the value in an alternative product then it may be a more effective promotional tool than a marketing campaign where costs are ultimately borne by consumers. Using real time product data, ADRs would be able to make recommendations to consumers about new offerings[51], possibly in real time.

Increasingly, data holders are becoming ADRs themselves. As the CDR grows, data holders will be able to create opportunities to expand their business by receiving data as well as providing it. Current and prospective data holders have expressed interest in the cross-platform opportunities provided by the CDR – as data holders and data recipients – and the potential for a successful CDR to draw additional investment to Australia.[52] One simple use of telecommunications data that could be explored is the use of customer data to validate or verify identity with consent. Identity verification is an issue when onboarding customers from various sectors, so more consistent and available data points may assist.

An ADR that normally operates outside the sector may add value to the telecommunications market by informing consumers about new services that are being offered. As noted by Optus, 'competition in the mobile market is driven by investment and innovation, with mobile carriers investing in extended coverage and better capacity'.[53] If CDR data sharing provides faster and more accurate information about improved services to consumers, then those carriers that invest and innovate will be better incentivised and rewarded for their efforts.

Greater opportunities for innovation will be unlocked as the CDR is extended to more sectors. Cross sector data will enable consumers to compare bundles made up of products from multiple sectors and use apps that combine data from multiple sectors to provide consumers with an accurate and more complete picture of their spending and finances. The Telecommunications Industry

[49] AGL submission, p. 1.
[50] ACCC submission, p. 10.
[51] Ibid, p. 10.
[52] Australian Financial Review, 2021, *Consumer data right will break down traditional industry silos: ANZ,* 16 September 2021
[53] Optus submission, p. 4.

Ombudsman's recent *Responding to consumers in financial hardship* report[54] suggests there can be room to improve how telecommunication providers engage with consumers struggling with their finances.

Sharing location data with ADRs has significant potential to allow the development of innovative services tailored to a consumers' location.

Substitutes for location data held by carriers must also be considered when weighing up the benefits of potential innovation. Personal location data comes from a variety of sources, including GPS, sensor data from a user's mobile device and carrier mobile towers. Telecommunications providers using information about a phone's proximity to mobile towers can triangulate signal strength to approximate the phone's location. Geolocation data is also collected by digital platforms, apps, and mobile operating system providers to a more accurate degree[55], and is already being shared by consumers with increasing levels of awareness. Further issues in relation to location data are discussed in the privacy impact assessment at Attachment A. Location data should not be designated under a telecommunications CDR at this stage.

4.4 Privacy and confidentiality

CDR privacy and confidentiality protections

The CDR legislative framework has in-built privacy and security protections including the 13 Privacy Safeguards under the Act as well as rules that relate to the privacy and confidentiality of CDR data. The Privacy Safeguards apply to consumer data and set out privacy rights for consumers and obligations for participants (such as data holders who disclose CDR data and ADRs, who collect and use CDR data). The Privacy Safeguards and rules include requirements for obtaining informed consent to collect, use and disclose CDR data (including providing CDR consumers with control over the types or subsets of CDR data that is shared and to whom and for what purpose), obligations around the quality and integrity of consumer data, obligations for the security of CDR data (including in relation to when CDR data must be deleted or de-identified and how), and a data minimisation principle.

In addition, under the framework, parties that can collect CDR data from data holders (and then use that data) must be accredited. Accreditation indicates that a party has met the strict accreditation criteria and makes that party accountable for their use and disclosure of CDR data. The Data Recipient Accreditor (currently, the ACCC) can accredit persons if they meet criteria regarding insurance, being a fit and proper person, information security, and appropriate internal and external dispute resolution processes.[56] The conduct of ADRs (as well as data holders) is also overseen by the ACCC and the OAIC. In particular, the OAIC is responsible for enforcing the Privacy Safeguards and consumer data rules that relate to those safeguards or to the privacy or confidentiality of CDR data, and provides complaint handling for these matters.

---

[54] Telecommunications Industry Ombudsman, *Responding to consumers in financial hardship*, Systemic Investigation Report, September 2021. Accessed 10 September 2021 at: https://www.tio.com.au/sites/default/files/2021-08/TIO_Systemic_Report_Responding%20to%20Consumers%20in%20Financial%20Hardship_fa_HiRes%20%28f1%29.pdf,

[55] Telstra submission, p. 12.

[56] Treasury 2021, *Payments system review,* available from: https://treasury.gov.au/sites/default/files/2021-08/p2021-198587.pdf.

By providing a secure framework to share data, the CDR provides a greater level of privacy protection and security to consumers than is afforded by other data sharing methods that are currently used outside of the CDR. For example, the CDR is a safer alternative to screen scraping, which requires consumers to provide their banking username and password to a third party to receive services, and to consumers sharing their information via email. Accordingly, if the telecommunications sector is designated, the CDR will uplift the security and privacy of data sharing for consumers that choose to share telecommunications data and use the regime.

Impact of telecommunications designation on privacy and confidentiality

A privacy impact assessment (PIA) that considers the privacy impacts of datasets raised in consultation and other general privacy considerations associated with designation of the telecommunications sector is at Attachment A. PIAs were previously conducted on the proposed implementation of the CDR regime in the banking and energy sectors. The telecommunications designation PIA supplements and builds upon the analysis contained in these reports and focuses on privacy issues specific to designating the telecommunications sector. At the rule-making stage, a further PIA would be conducted.

The PIA considers the potential impact that designation of the telecommunications sector may have on individuals' privacy as required by the *Privacy (Australian Government Agencies – Governance) APP Code 2017*. The same considerations do not apply to the confidentiality of business data. However, where the sharing of business data could have an impact on individual privacy, this has been considered as part of the assessment. The overall security of CDR data under the regime is also an important consideration when it comes to protecting confidentiality of business information. Privacy safeguard 12 and the CDR rules set out the minimum steps that ADRs must take to protect CDR data, and ensures that data is protected to a high standard and the capability of an ADR's security posture is regularly reviewed.

We consider the privacy risks associated with the datasets proposed for designation are not of a nature that should prevent those datasets, nor the telecommunications sector more generally, from being designated. This PIA identifies privacy issues that will be given further consideration at the rule-making stage. Also considered in the PIA are the privacy risks associated with certain datasets that are not proposed for designation, but which were raised by stakeholders during consultation. These privacy considerations factored into Treasury's assessment of whether to exclude these datasets from the proposed scope of designation.

4.5 Intellectual property

Designation instruments for the banking and energy sectors exclude 'materially enhanced information' about the use of a banking product and the sale or supply of electricity from being specified classes of information subject to the CDR regime. The concept of materially enhanced information refers to data that is the result of the application of insight, analysis or transformation to significantly enhance its usability and value in comparison to its source material. Data holders cannot be required to disclose materially enhanced data about the use or sale/supply of products under the CDR but may be authorised to disclose it through the CDR on a voluntary basis. Specific intellectual property issues were not raised in the consultation process in relation to the telecommunications datasets considered, however, a similar approach to excluding materially enhanced information would be taken if the telecommunications sector is designated. The

opportunity to provide input on the concept of materially enhanced information will be provided as part of consulting on any draft designation instrument.

4.6 The public interest

The CDR gives individuals and businesses more control over their own data, enabling them to safely, efficiently and conveniently harness information about themselves for their own benefit. The CDR is a key component of the government's Digital Economy Strategy, which envisions Australia as a leading digital economy and society by 2030. The potential benefits to the Australian economy through digitalisation have been estimated to be as much as $315 billion over the next decade[57] and will benefit all aspects of Australian society. The CDR will establish the foundations of the data economy, creating new opportunities for Australian consumers and data-driven businesses to develop better products and services.[58]

Australia is the first country to have established and commenced implementation of an economy-wide consumer data portability framework. As an economy-wide reform, the CDR will allow the combination of data from different sectors to create opportunities for innovative use cases that add convenience and control to consumers' lives, support economic growth and create new high value jobs. The CDR could also support an interoperable and rules-based approach to international consumer data portability and sharing frameworks[59], supporting opportunities for Australian businesses to provide innovative data-driven services in a global marketplace.

The efficiency and effectiveness of Australia's telecommunications sector is critical and integral to the lives of almost all Australian consumers and an essential input for most businesses. Telecommunications services are at the centre of household social and economic participation, particularly in the context of the COVID-19 pandemic which has led Australians to rely more heavily on their broadband services for work, education, entertainment, telehealth and other services [60] – especially in regional areas. The ubiquity of telecommunications services in our lives means small benefits achieved in the delivery of, and consumers' access to, these services will spread throughout the economy.

Application of the CDR to telecommunications can enhance the economic wellbeing of Australians by improving product comparison and assisting consumers to switch to better value deals that match their needs and possibly reduce their telecommunications spend. Lower monthly telecommunication costs could impact the living expenses of many Australians, particularly low-income households. Designation of the telecommunications sector under the CDR will drive better consumer decisions and further incentives for service providers to deliver enhanced telecommunications services to support the digital economy.

[57] Australian Government, 2021. *Australia's Digital Economy.* Available at: https://digitaleconomy.pmc.gov.au/strategy/executive-summary
[58] Australian Government, 2021. *Australia's Digital Economy.* Available at: https://digitaleconomy.pmc.gov.au/strategy/executive-summary
[59] Australian Government, 2021. *Australia's Digital Economy.* Available at: https://digitaleconomy.pmc.gov.au/strategy/executive-summary
[60] ACCC.2020, *ACCC Communications Market Report 2019-20*. Available at: ACCC Communications Market Report 2019-20 December 2020

4.7 Regulatory Impact

Designation is a threshold decision that captures data holders and datasets for participation in the CDR but does not itself impose regulatory obligations on data holders. As such, assessing regulatory impact at the designation stage involves considering potential compliance costs in a general and high-level way, and using assumptions to produce estimates.

Treasury sought feedback on regulatory impact in the consultation paper and later engaged the consultancy Grant Thornton to assist in preparing a report on regulatory impact based on a further round of targeted stakeholder consultation. Grant Thornton's report on the regulatory impact of the proposed scope is available at Attachment B.

The relative preparedness of the telecommunications sector for the CDR was considered during consultation. The general consensus was that stakeholders have not yet fully planned for and costed the impact of CDR designation. Feedback suggested there are particular features of the telecommunications sector that contribute to this level of preparedness. The sector has a large number of providers and many are small operators. The sector has experienced numerous mergers and acquisitions in recent years, for which IT consolidation projects are still occurring. Retailers in the sector tend to have a large product set because of constantly developing technologies. Similar to issues affecting banking and energy sectors, the telecommunications sector carries legacy IT systems and has needs for general system upgrades.

Grant Thornton provided estimates of what data holders might spend to become compliant with the CDR. The estimates are highly caveated given they are based on consultations with stakeholders before the development of the rules and standards that are necessary to support implementation of the CDR in the telecommunications sector. At this point in the sectoral assessment process, the retailers consulted were unable to provide specific data related to the potential cost implications of designation. More specific information was provided by vendors consulted given their experience in the banking sector to date.

The estimates are based on the assumption that choices are made at the rules stage that minimise regulatory impact. They do not take into account costs involved in organisation-wide digital transformation projects to update legacy IT systems. They also assume outsourced service providers are available to support data holders to efficiently comply with their CDR obligations, for either or both of product reference data and consumer data sharing obligations. The estimates are based on the proposed scope of designation in this report and do not take into account the diversity and complexity of retailers in the sector, necessarily simplifying the sector into two categories (large and small providers):

- Small telco (Year 1 – Build): $340,000
- Small telco (Year 2 – Run): $160,000
- Large telco (Year 1 – Build): $4,300,000
- Large telco (Year 2 – Run): $1,280,000

Build costs include discovery and the expense of building new systems and/or adapting existing systems to share the types of consumer and product data outlined in the proposed scope of designation. Run costs include yearly subscription costs to outsourced service providers and internal run costs.

We consider the estimated costs plausible and note a more accurate and detailed estimate of regulatory impact will be explored at the rule-making stage.

Further, the insights provided at this stage in the process can assist to ensure regulatory costs are minimised at the rule-making stage. For example, as highlighted in the Grant Thornton report, different implementation options may have a higher or lower regulatory impact. Regulatory burden could be reduced by minimising the number and complexity of the datasets ultimately required to be shared, and even minimising the number of data holders mandated to share it. Other lower cost options could exclude certain enterprise or complex customer accounts, or provide for a phased rollout by the size of retailer, complexity of product or customer type, or type of dataset.

5. Approach to designation

5.1 Recommended datasets

Designation of the telecommunications sector that would support data sharing is recommended with:

- product information that is already publicly available;
- product information that is specific to the product used by an eligible CDR consumer; and
- basic consumer and account data, such as data available to consumers on their bills or through online accounts or mobile apps.

Having regard to the nature of designation, it is therefore recommended the following classes of information be designated and for reference purposes include examples of the types of data sharing this could support at the rule-making stage.

Class of information	Scope of class	Relevant data holder/s of the information	Potential required datasets in CDR rules for telecommunications sector
Product information[61]			
Information about retail offers or supplies of products	Information about products including information that: • identifies or describes such products • is about the price of, or fees and charges associated with, such products	Carriers[62] Carriage service providers[63]	Designating this class of information would enable the CDR rules to impose mandatory obligations for data holders to share what is commonly referred to in the CDR regime as 'generic product reference data'.

[61] Product data is subject to limitations set out in section 56BF of the Act and is data for which there are no CDR consumers.

[62] Includes all those who hold carrier licences to own and operate telecommunications networks units or have assumed carrier obligations (for example, under a nominated carrier declaration) to operate telecommunications network units on behalf of a non-carrier owner to the extent they publicly offer retail products to consumers.

[63] Includes retailers of telecommunications services, including resellers of services provided by carriers, for example, mobile virtual network operators.

Class of information	Scope of class	Relevant data holder/s of the information	Potential required datasets in CDR rules for telecommunications sector
	• is about the terms and conditions of such products • is about the term or duration of such products • is about bundling associated with such products • is about services that are available for such products for customers that require additional assistance such as customers with disability • is about priority assistance services that are available for such products.		In the telecommunications sector, product reference data is likely to include the type of information typically included in a Critical Information Summary[64] or in a Key Facts Sheet[65].
Consumer information			
Information about retail offers or supplies of products (as above) as it relates to a particular product used by a consumer	The product information described above.	Carriers Carriage service providers	Designating this class of information would enable the CDR rules to impose mandatory obligations for data holders to share what is commonly referred to in the CDR regime as 'product specific data'. Product specific data enables product data to be shared as a type of consumer data. For example, if a consumer is on a particular price that differs from the advertised price of a product, or uses a product that is no longer publicly available, that specific product information that relates to the

[64] Under the Telecommunications Consumer Protections Code, a service provider must provide consumers with a PDF 'Critical Information Summary' for each offered product, service, and plan, setting out key information about what's included and excluded, and terms and conditions.

[65] Telecommunications (NBN Consumer Information) Industry Standard 2018 requires internet service providers to provide consumers with a 'Key Facts Sheet' before they purchase an NBN service, including information about speeds.

Class of information	Scope of class	Relevant data holder/s of the information	Potential required datasets in CDR rules for telecommunications sector
			product a consumer uses could be shared as consumer data. With regards to services for customers that require special assistance or priority assistance, sharing product specific data about these attributes of products (if the rules required this) would not involve sharing the fact that a consumer makes use of such services – simply whether the services are available for the particular product used by a consumer.
Information about retail customers and users	Information about a customer or user of a telecommunications service, including information that person has provided to the supplier of the service (or another person on behalf of the supplier) in connection with the supply or use of the service.	Carriers Carriage service providers	Designating this class of information would enable the CDR rules to impose mandatory obligations for data holders to share what is commonly referred to in the CDR regime as 'customer data'. In the banking and energy sectors, at the rule-making stage, this has included basic contact details like name, address, and phone number. Under the current CDR rules, date of birth has not been included.
Billing and account information about retail supplies of products	Including: • information about accounts such as account numbers and product usage or data usage relating to the account • information about bills issued such as billing periods, invoice numbers, date of issue, current and previous balances, due dates, and details of	Carriers Carriage service providers	Designating this class of data would enable the CDR rules to impose mandatory obligations for data holders to share information typically available to consumers on service bills, or otherwise information that is associated with a customer's account and that they would be able to access.

Class of information	Scope of class	Relevant data holder/s of the information	Potential required datasets in CDR rules for telecommunications sector
	how to make payments • information about arrangements for payments to be made in response to such bills (such as direct debit details, details about online payments and BPAY details) • information about payments or government concessions or rebates provided in connection with the supply (such as details of previous payments, dates of direct debits, details about phone handset payments and receipt numbers) • other information about such supplies that is used for the purposes of billing (such as which plan the customer is on, telephone numbers to which the bill relates, fees and charges, discounts applied, and, for the different services offered under the product, summaries of product usage and data usage for the billing period and associated costs) • information about how long until a contract relating to a particular product is due to end.		

5.2 Data not recommended for designation

The consultation paper explored a wide range of datasets (and data holders) in terms of a potential designation of the telecommunications sector. Following consultation and consideration of the

statutory factors, we consider that there are several datasets and potential data holders that should not be included for initial designation. However, we also consider that there are some types of data that could be considered for potential designation in the future.

Item	Reasons for initial exclusion
Data holders	
Providers of 'over the top' (OTT) communications services	While OTT services are playing an increasing role in providing services to consumers traditionally associated with the telecommunications sector (such as messaging and voice calls), they are simply one use of telecommunications data provided to consumers by retail service providers. These services are evolving rapidly, and it would be appropriate to consider their potential designation as data holders at a later time and in the context of other sectoral assessments relevant to sectors in which OTT providers (and similar entities) principally operate.
Network providers	There are a range of issues relating to broadband speed data that mean that this class of data would not be appropriate for designation at this time. If telecommunications carriers are designated in accordance with the proposed scope, those only providing a network for wholesaling purposes (including NBN Co) would not be data holders in practice as they do not hold the information proposed for designation or publicly offer products to consumers.
Product data	
Mobile coverage data	Data relating to the predicted level of coverage available to consumers using a particular carrier, in a particular area, may be useful for product comparison. However, the information currently provided in published coverage maps is not standardised and the accuracy of the information can vary depending on a range of factors. In the future, if there is more standardisation in publication of this data, it could be considered for designation under the CDR.
Consumer data	
Content or substance of communications	The content or substance of communications can contain highly sensitive information about a person who is party to a communication and raises increased privacy risks compared to the kind of data already being shared in the CDR regime and the kind of data being proposed for designation in this report. Under the *Telecommunications (Interception and Access) Act 1979*, access to data that is effectively the content and substance of a communication is only permitted by law enforcement agencies in extremely limited circumstances. While privacy impact is one of the statutory factors to be considered among others in making a designation decision, submissions to the consultation paper did not present use cases for this type of information and, at this stage, it has not been established that the benefit to consumers of sharing this type of information outweighs likely privacy risks. As a result, we recommend this dataset be excluded from designation.
Location or phone cell tower data	Data held by carriers that relates to the location of a consumer (or the location from which a consumer makes communications or uses communication services) should be excluded from designation at this time. This is based on consideration of the privacy risks and potential harm if the information is misused, together with the accuracy of the data. Location data held by carriers with respect to the location of communications is by reference to network equipment location (for example, tower location for mobile services) and is of variable accuracy depending on the network equipment used (for example, mobile network location data derived from radiocommunications equipment is not considered to be as accurate as satellite network derived GPS data).

Item	Reasons for initial exclusion
	Therefore, we do not consider that the telecommunications sector is best placed to provide location data. We consider there may be significant consumer and innovation benefits from sharing location data (provided adequate protections are in place), however, benefits may be greater for more accurate kinds of location data. Designation of this type of consumer data could be considered further at a later stage.
Broadband speed data	We recommend not designating NBN broadband speed data in its current available form. NBN Co does hold data relating to actual and attainable speeds achieved on their network, however, the utility of this information is limited as it does not provide a complete picture of a customer's experience which is affected by various operational factors across the supply chain, and external factors beyond the control of wholesale providers or retailers. Broadband speed data held by carriers is incomplete and no industry standards exist to ensure regular collection. If available, the sharing of this data in its current form and scope could lead to unintended consequences as the underlying performance factors are open to misinterpretation and could be impacted by the evolution of the broadband market.
Information about the existence of financial hardship arrangements	The potential to designate information about financial hardship arrangements in telecommunications was raised in the consultation. Privacy concerns were raised about this information revealing sensitive insights into a consumer's financial capacity, which could influence the goods and services subsequently offered to them. There may be some consumer benefits from including hardship information in a designation, for example, it may be shared with a trusted third party such as a financial counsellor to provide financial advice and support. However, there was a lack of evidence about the benefits of using this information outweighing risks to privacy and discrimination. At this stage, it is not recommended that hardship information is designated. However, this could be revisited in the future if compelling use cases emerge and appropriate mitigation strategies to address the sensitivity of this information are considered.
Materially enhanced information	Exclusion of materially enhanced information would be consistent with the approach taken in the banking and energy sectors and align with the general principle in the CDR to date that data holders should not be required to share information that has significantly enhanced usability or value compared to its source material due to the application of proprietary insight or analysis.

5.3 Matters recommended for consideration relating to the CDR rules

A broad range of issues relating to the implementation of the CDR in the telecommunications sector were commented on by stakeholders in submissions and discussions that will be appropriately addressed (and consulted on further) in the rule-making stage. This is consistent with the role of the designation instrument and CDR rules in the CDR regulatory framework and the current approaches applied in considering similar issues in the banking and energy sectors.

Further public consultation will occur at the rule-making stage (which is expected to occur concurrently with development of data standards for the sector) to inform implementation design and obligations in the rules. Further privacy and regulatory impact analysis will occur.

Data required to be shared

The rules will specify the datasets that are required to be shared with more specificity and within the bounds of designation. However, a couple of datasets – that may be covered by the scope of designation –are not appropriate to share at this time. If these datasets are shared in the future, further regulatory impact and privacy impact assessments would be required.

Performance or quality of service data

The scope of designation may include information that data holders may hold about the performance or quality of service regarding a particular product (for example, connection or response times, or complaints data). We did not identify data that could be required to be shared at this stage. However, if standardised and publicly available performance data emerges over time, we consider the CDR rules could undertake the necessary consultation to establish whether this information could be shared to support product comparison on non-price elements of telecommunications services.

Called party numbers

The scope of designation may also include information about third parties. Details such as who specific communications were made to ('called party numbers') are typically available on bills. Privacy concerns have been raised about the potential for this information to reveal personal information about the CDR consumer and third parties who may not have provided consent. However, there may be innovative use cases that this data could support, particularly for small business management and administration purposes. Further consideration should be given to including this information as well as potential mitigation strategies to address the privacy risks at the rule-making stage. However, rules should be made that do not allow this information to be shared in the first instance.

Eligible CDR consumers

Telecommunication services are used by individuals and entities with account holders ranging from large corporations to minors (in certain jurisdictions). The potential uses and risks of sharing designated telecommunications data will vary from customer to customer. The CDR rules contain a cross-sectoral concept of 'eligible CDR consumer' (being a CDR consumer that is eligible to make data sharing requests), however, this can be modified on a sector-specific basis as required. At the rule-making stage, this could be further considered for the telecommunications sector, including whether specific consumer cohorts could be assessed to inform the boundaries drawn in the rules.

Enterprise customers

In some telecommunications market segments, such as the enterprise market, there may be customers with highly customised contracts and arrangements. Where the specific terms of these contracts are not publicly available, they will not be captured under generic product data sharing obligations. Enterprise customers often approach retailers to negotiate their own contracts, so the utility of public product data for them is limited. In many instances our regulatory impact assessment analysis revealed that enterprise customers are serviced through separate IT systems, which would increase CDR compliance costs for industry participants should they be required to share consumer data for these customers. If the sector is designated, when defining who is an 'eligible CDR consumer' in the rules for the telecommunications sector, consideration should be given to differentiating between enterprise customers with bespoke arrangements and those on standard-form contracts (for example, individual consumers and small businesses) while also seeking

to ensure that as many business customers as possible can use the CDR. Delineations between these market segments already exist in the telecommunications sector that could be considered for the purposes of an eligibility threshold; for example, the Telecommunications Consumer Protections Code, which distinguishes between consumers that spend more or less than $40,000 on services).

Phasing of data sharing obligations

The rules specify when mandatory data sharing obligations commence for data holders. Based on existing precedents in banking and energy, commencement of obligations may apply in phases by reference to different data holders, different datasets or by reference to particular functionality. For example, in the banking sector, the 4 major banks were required to commence sharing data earlier than other authorised deposit-taking institutions, and commencement dates for sharing particular datasets have been phased. This is a mechanism that enables sector participants to manage implementation and technical build programs, resources, and delivery risks.

Smaller providers

In addition to phasing commencement obligations, the likely regulatory impact of obligations is a key consideration at the rule-making stage in relation to potential exclusion from mandatory obligations for some sector participants (for example, by reference to customer thresholds or financial size).

There are approximately 250 smaller telecommunications providers in the 'long tail' of the market.[66] ACCAN notes the role of smaller players and how CDR designation could impact their costs and market visibility:

> Telecommunications micro-providers who lack the technical capacity to be data holders may need to be excluded from data holder responsibilities to enable them to compete against larger telco providers as part of the CDR system. Excluding smaller providers from the CDR on the basis that they are not data holders could result in provision of inaccurate comparative advice to consumers, and undermine the intention of the CDR.[67]

The marginal cost of complying with CDR consumer data sharing obligations could discourage smaller entrants to the market. However, requiring provision of product data only under the CDR may enable smaller providers to compete more effectively through product comparison. Consideration of this issue at the rule-making stage is appropriate to enable further regulatory impact analysis to occur in relation to proposed obligations, and to ensure that voluntary participation of all sector participants will be possible (as designated data holders) even if a mandatory participation threshold applies.

White labelling in the telecommunications sector

White label products are typically supplied by one entity (a white labeller) and branded and retailed to consumers by another entity (a brand owner). White labelling is a feature of a number of products in the telecommunications sector, including mobile and broadband plans. In telecommunications, white labellers are often both retailers and wholesalers. These carriage service providers would likely be data holders for the data they hold in respect of a white label product, and potentially subject to data sharing obligations under the CDR rules if the sector is designated. In some instances, the carriage service provider may hold the relevant data. In other instances, the

[66] Communications Alliance submission, p. 6.
[67] ACCAN submission, p. 10.

brand or retailer may hold the relevant data, for example, if the brand manages billing and the customer relationship.

Once the telecommunications sector is designated, the CDR rules and standards (and related guidance) will address where data sharing obligations sit in a white labelling scenario, and the extent that those obligations need to be made transparent to consumers. Just as in the banking sector, consideration would need to be given to having sufficient flexibility to support the various white labelling scenarios that exist in the telecommunications sector. Such data sharing would also be subject to the phased implementation considerations, noted above.

Part 13 of the Telecommunications Act

Part 13 of the *Telecommunications Act 1997* (Cth) (Telecommunications Act) sets out requirements for carriers, carriage service providers and others related to the telecommunications sector regarding use and disclosure of information in relation to communications (including individuals' personal information). It is an offence for eligible persons to disclose or use information protected by Part 13, otherwise than for a purpose specified in the Telecommunications Act or as otherwise authorised by law.

There is likely to be a degree of overlap between Part 13 protected information and information that may be designated under a telecommunications CDR. Whether Part 13 could prevent the disclosure and use of information under the CDR was raised during consultation. While developing rules for a telecommunications CDR (if designated), consideration will be given, in consultation with the Minister for Communications, Urban Infrastructure, Cities and the Arts, to ensure data sharing obligations under the CDR regime operate consistently with the primary and secondary use and disclosure obligations under Part 13 of the Telecommunications Act. In the course of developing rules for a telecommunications CDR (if designated), consideration will be given, in consultation with the Minister for Communications, Urban Infrastructure, Cities and the Arts, to ensure data sharing obligations under the CDR regime operate consistently with the primary and secondary use and disclosure obligations under Part 13 of the Telecommunications Ac

Attachment A: Telecommunications sectoral assessment – privacy impact assessment (PIA)

Executive summary

We consider the privacy risks associated with the datasets recommended for designation are not of a nature that should prevent those datasets, nor the telecommunications sector more generally, from being designated. This privacy impact assessment (PIA) identifies privacy issues that will be given further consideration at the rule-making and standard setting stages, and a further PIA would be conducted at the rule-making stage. The PIA also considers privacy risks associated with certain datasets raised in consultation that are not proposed for designation. These privacy considerations were factored into Treasury's assessment of whether to exclude these datasets from the proposed scope of designation. Lastly, this PIA considers general privacy issues raised during consultation that are not specific to particular datasets.

Part I: Privacy impacts associated with the proposed scope of designation

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
Designation of information about retail customers and users				
1.	Information about a customer or user may encompass a broad class of data including information that identifies an individual, such as contact details, and other information that an individual has supplied to a data holder about themselves.	While this information (categorised as 'customer data' under the CDR rules for banking and energy) is often required to be shared to identify or contact a consumer, if the information is accessed by an unauthorised person it could be misused and impact an individual's privacy; for example, for direct marketing purposes. In submissions to the consultation, the OAIC identified mobile porting fraud[68] as an existing security issue in the telecommunications sector that the application of the CDR may impact	The risk of customer data being used inappropriately is mitigated by the CDR accreditation process, under which third parties must meet rigorous privacy and security requirements before they can receive and use CDR data from data holders. These requirements must be maintained when a person has become accredited, and include implementing a security governance framework, maintaining a comprehensive information security capability, managing and reporting security incidents, and strict requirements around who has access to data within an ADR's CDR data environment. There are also strict requirements around who an ADR can disclose CDR data to, including outsourced	Customer data has been designated under the banking and energy designation instruments and is currently being shared in the banking sector (it is required data for the purpose of mandatory data sharing obligations). We consider the privacy impact of including customer data in a telecommunications designation (with a view to customer data being required data under the rules) would be appropriately mitigated by the CDR's rigorous accreditation process and ongoing obligations on accredited persons, which ensure that ADRs have robust privacy and security measures in place to protect against the unauthorised access to or misuse of customer data. Mobile porting fraud was identified as an industry-specific security concern during consultation. A key

[68] This refers to a practice in which scammers use stolen identity information to fraudulently port mobile numbers, enabling them to complete security verification for linked accounts such as banking or social media.

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
		(discussed further below under sector specific risks, row 11).	service providers and trusted advisers of consumers in particular circumstances. Under the *Competition and Consumer Act 2010* (the Act), ADRs must comply with the 13 privacy safeguards which relate to collection, management, disclosure and use of CDR data. The privacy safeguards prohibit ADRs from direct marketing to consumers unless they have specific consumer consent (as required by the CDR rules) to do this. A breach of the privacy and security protections in the regime can result in enforcement action being taken against the relevant ADR for non-compliance of civil penalty obligations. The ACCC and OAIC have a joint CDR Compliance and Enforcement Policy and complaints about data handling can also be lodged with the OAIC. Strong individual authentication requirements are embedded in the CDR data sharing process with strong customer authentication required for data holders to authenticate CDR consumers, before they can disclose CDR data to an ADR.	mitigant against this risk is strong customer authentication, and we note that recent regulatory reform in the telecommunications sector has sought to strengthen authentication management by mandating stronger identity verification processes for telecommunications service providers.[69] We recommend the PIA at the rule-making stage consider any measures that could further mitigate the risk of identity fraud.
Designation of information about retail supplies of products				
2.	Information about such supplies that is used for the purposes of billing may include summaries of data usage ('usage data'). Under this	If designated and required to be shared under the CDR rules, usage data could be analysed by ADRs in a way that would make it possible to draw insights about the CDR consumer or other people.	An ADR must only use CDR data in accordance with a consent given by a CDR consumer, meaning the ADR may only draw inferences about a CDR consumer if they have given express and informed consent for the ADR to do so as part of requesting a particular good or	Overall, we consider the privacy risks associated with designating usage data can be appropriately managed through application of the existing mitigation strategies in the rules. We recommend further consideration at the rule-making stage in relation to the need for any additional rules.

[69] *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020*.

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
	designation, rules could be made that require information such as the total number of calls or SMSs, or total amount of data used over a certain period, to be shared.	For example, usage information may indicate high gaming or streaming use, which may make it possible to draw insights about, for example, how many people are living in a household. Patterns of data and rates of usage at specific times of day or on weekdays may indicate, for example, when a CDR consumer is commuting to work.	service from the ADR. Under the CDR rules and customer experience (CX) standards, there are strict requirements on ADRs seeking consent including to make sure that the consent is specific, express and informed. The CDR rules prohibit ADRs from requesting consent to use CDR data for the purpose of identifying, compiling insights in relation to, or building a profile in relation to any identifiable person who is not the CDR consumer making the consumer data sharing request.[70] In addition, ADRs are accredited persons who have undergone a rigorous process to establish that they have met the accreditation criteria, which includes a fit and proper person criterion. The ACCC and OAIC, as regulators of the CDR, enforce the CDR legislation and rules including enforcement of strict consent rules, permitted uses and disclosures, and compliance with rules generally.	We consider that the usage data that is currently available to consumers through bills or mobile apps could be appropriately required to be shared at the rule-making stage based on the existing privacy and security framework in the CDR regime. Usage data is already provided to consumers through bills from service providers and in most cases, is also available via online accounts and applications (including for download). Consumers already provide this usage information through less secure means than the CDR to third party comparison services to enable the service to match a product or service to their usage needs. Designating usage data is consistent with the principle that consumers should be able to share through the CDR information they are already able to view and access, to derive benefits from it through sharing with ADRs. As consumers already have access to this data, we do not consider the potential for its secure transfer with informed consent under the CDR regime raises specific privacy concerns that are not already present and are not able to be mitigated by the CDR rules and standards (including CX standards). We recommend further consideration of the impact of inferences being drawn from usage data, as well as strategies to mitigate any consumer harm, be given at the rule-making stage.

[70] *Competition and Consumer (Consumer Data Right) Rules* 2020, r4.12(3)(b)(iii)

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
3.	Information about such supplies that is used for the purposes of billing may include information about third parties. For example, a phone bill may contain details of whom specific communications were made to ('called party numbers').	Called party numbers and other information about where a call or data transaction terminated may reveal personal information about a third party as well as information about the caller (for example, how frequently a third party is contacted by a CDR consumer). Because a called party number provides a means of contacting an individual directly, sharing called party details may have a privacy impact on the called party, for example, if the information was used to make inferences about that person, or to contact that person.	The existing rules prohibit ADRs from requesting consent to use CDR data for the purpose of identifying, compiling insights in relation to, or building a profile in relation to, any identifiable person who is not the CDR consumer who has made a consumer data sharing request. An ADR is not permitted to use CDR data except for in accordance with a valid consent. In addition, the rules include a 'data minimisation principle' which ensures CDR data is only collected and used if it is necessary to provide the good or service a consumer has requested. Therefore, information about a called party cannot be collected and used if it is superfluous to the good or service ultimately being delivered to the consumer.	The CDR regime already captures data that might reveal information about a third party in other sectors (for example, in the banking sector, information such as BSB numbers, names and account numbers may be disclosed as part of a consumer's payee list) and mechanisms within the rules exist to mitigate the risks associated with sharing this information. We recommend the PIA at the rule-making stage examine additional mitigation strategies as necessary to address any privacy issues associated with sharing information about third parties that are unique to the telecommunications sector (should this information be included for sharing under the rules). The data standards could ensure that call party numbers are in a separate data cluster (if in scope in the future), such that consumers would need to give specific consent to their collection and to assist in compliance with the data minimisation principle.
4.	Billing information about retail supplies of products includes information about government concessions or rebates provided in connection with the supply. A concession could include a discount or rebate on a customer's bill because the	Information about concessional arrangements may reveal sensitive insights about a consumer, for example a consumer's age or financial capacity.	The consent rules ensure that consumers give informed and express consent to the collection and use of their data, and this includes actively selecting which data they share and for what purposes. Any sharing of information about hardship arrangements or other concessional arrangements would be subject to the existing rules around consent. This includes the requirement that the information is actively selected and the consent to share it is informed and not bundled in with consents for other, less sensitive categories or sub-categories of CDR data.	There are existing mitigation strategies for this kind of data already in place in the CDR regime and subsequent rule and standards making processes that could address the privacy impact of sharing this information – for example, through ensuring that concessional information is presented as a standalone data cluster or type of data that consumers must actively select to share during the consent process, and ensuring that processes for consent to collect and use this particular dataset are sufficiently transparent to enable a consumer to make an informed decision about sharing it. This will ensure that CDR consumers are given sufficient

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
	customer is eligible for a government concession (such as a pensioner concession) or relief scheme.		The standards could ensure that information about concessions could be presented as its own data cluster in the consent process.	control over whether to share this information about themselves. Given the existing mitigation strategies to manage the privacy impacts associated with designating information about concessional arrangements and the likely utility of including this information in the CDR regime (as outlined in the report), we recommend that this information be included in the designating instrument.
5.	Information about retail supplies used for the purposes of billing may include some types of metadata such as the source, destination, date, time, duration, type and location of a communication.	Submissions raised significant privacy concerns about the possible designation of information commonly referred to as metadata.[71] The OAIC considers that metadata can provide information about individuals' relationships, networks and frequently visited locations. This can map out an individual's intentions through pattern recognition of their daily habits and movements. Conclusions that may be inferred from metadata may also reveal sensitive information about the individual (such as information about an individual's health, political opinions, sexual orientation and circumstances of vulnerability). The OAIC does not consider express	The consent rules ensure that ADRs are required to obtain informed consent from CDR consumers in relation to the collection and use of their data, and this includes actively selecting which data they share and for what purposes. ADRs are restricted in how they can use CDR data and only permitted to use the data in accordance with a consumer's consent. Therefore, if metadata were designated and ultimately required to be shared under the rules, a consumer would need to voluntarily give informed consent to its collection and use and ADRs could be subject to enforcement action by the regulators (ACCC and OAIC) for using the data in ways that do not accord with the consumer's informed consent. In addition, the rules include a 'data minimisation principle' which ensures that CDR data is only collected and used if it is necessary for the provision of the good or service the	On balance, the privacy impact associated with sharing the type of metadata commonly available on/associated with a bill is not sufficient, in and of itself, to necessitate the exclusion of information about a communication as a designated class of information. Which specific metadata datasets would be subject to mandatory data sharing obligations (if any) will be determined at the rule-making stage. Designation of billing information would facilitate, at the rule-making stage, metadata of the kind provided to consumers on bills or invoices (such as dates and times of communications) to be made available through the CDR for the consumer's benefit. We recommend any consideration of whether to make rules requiring specific metadata datasets be shared be informed by further public consultation, regulatory impact assessment and privacy impact assessment at the rule-making stage.

[71] OAIC submission, p.4; AISA submission, p.3.

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
		consent would in and of itself mitigate the privacy risks of sharing metadata. The potential for harmful impacts can also be amplified for vulnerable consumers.[72] Under the mandatory data retention scheme, service providers are required to retain the location of equipment or a line used in connection with a communication, specifically for law enforcement purposes. The privacy impacts associated with designating carrier location data are dealt with separately below in Item 6.	consumer is receiving. Therefore, metadata could not be collected and used if it is superfluous to the good or service ultimately being delivered to the consumer.	

[72] OAIC submission, pp.4-5, 11.

Part II: privacy impacts of datasets excluded from proposed scope

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
6.	**Location data** Designation of information about location could, at the rules stage, ultimately include sharing of different types of location data that is held by a carrier.	Telecommunications providers receive information about a device's proximity to mobile towers (and other network equipment) by triangulation based on signal strength, approximate to the location of that device. Consumers are currently unable to access or share carrier location data that is relevant to the network over which their service/s are provided. The effect of designating carrier location data would be to provide consumers with access to a dataset they do not already have access to outside of the CDR regime. Location data can be highly sensitive in terms of what it reveals about a consumer or end user and their movements. This sensitivity increases with the specificity and precision of that data, for example, mobile phone tower location data arguably presents a slightly lower risk than satellite network provided GPS data, because the parameters of that location are larger. Key risks with sharing location data include that the data has the potential to disproportionately affect vulnerable consumers (especially if this location data is misused), and may include the	As for other classes of information mentioned above, any sharing of location data would be subject to stringent consent and use requirements under the rules. Regarding the potential for direct marketing based on location, the rules require a specific direct marketing consent to be given by the consumer for any direct marketing activities. The rules also include protections for situations of potential domestic or other violence. For example, data holders can refuse to disclose required consumer data without breaching the rules, where they consider it to be necessary to prevent harm or abuse.	Significant concerns have been raised about the possible privacy implications of designating location data held by telecommunications providers. Having regard to the range of statutory factors, including the potential privacy impact of designating this information and whether the consumer and innovation benefits could be more acutely realised if more accurate kinds of location data (for example GPS data) were designated at a future point, we recommend that location data not be included in the designation instrument for the telecommunications sector. If location data is designated at a later stage, we recommend careful consideration be given to whether, in addition to the existing mitigation strategies in the regime, supplementary rules or particular consumer experience standards for consent would be required to share this information to ensure consumer protection, particularly for vulnerable consumers.

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
		potential for discrimination based on location, the ability to ascertain location data about minors, direct marketing based on location, the ability to effectively conduct surveillance and predict historical patterns of behaviour, and location data being accessed by a perpetrator of domestic or other violence or crime to raise inferences about the whereabouts of a person at a particular time. Significant privacy concerns regarding the possible designation of location data were raised in submissions.[73] The OAIC considers that location data has a high privacy impact, as beyond showing where an individual has been, it can also reveal sensitive information about them such as their health and political or religious beliefs.[74] The OAIC also notes that it is difficult to make such data anonymous, and that the privacy risks associated with sharing location data would likely be increased where location data could be combined and analysed with other CDR data (for example, banking data).[75] The OAIC supports the existing consent framework in the CDR system, but		

[73] OAIC submission, p.8-11; Telstra submission, pp.11-12; AISA, p. 2; TIO submission, p. 1.
[74] OAIC submission, p. 9.
[75] OAIC submission, p. 9.

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
		considers express consent may not in and of itself be able to mitigate against the privacy risks of sharing location data.[76] The Australian Information Security Association (AISA) considers that location data is a 'risky' dataset and allowing consumers to consent to sharing such data places an unfair burden on the consumer to weigh the risk.[77] Stakeholders also raised concerns about the impact of sharing location data on vulnerable consumers, particularly victims of family and domestic violence, including the potential for location data to facilitate coercion and technology facilitated abuse.[78] These risks may be more acute in circumstances where an account has more than one user, and the additional users of an account are not the account holder (for example, in the case of a family or business plan).		
7.	**Content or substance of a communication** The *Telecommunications (Interception and Access) Act 1979* (TIA Act)	Stored communications are to some extent distinct from the telecommunications data required to be collected and retained by providers in compliance with the data retention regime under the TIA Act. Access to	As for the other categories in this assessment, the rules contain various mechanisms to ensure consumers are empowered and informed in choosing which data to record, store and share and for what purpose, and require ADRs to only use CDR data in accordance with consents	Under the TIA Act, access to data that is effectively the content and substance of a communication is only permitted by law enforcement agencies in extremely limited circumstances, due to the sensitive nature of this information. Stakeholders have also raised significant concerns about the

[76] OAIC submission, p. 10.
[77] AISA submission, p.2.
[78] ACMA submission, p. 5; p. 8; AISA submission, p.3; Telstra submission, p.9.

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
	prohibits interception of communications and access to communications either as they are "passing over a telecommunications network" or if they are stored communications[79] except with a lawfully obtained warrant. Part 13 of the Telecommunications Act 1997, prohibits telecommunications service providers from disclosing information gained about their customers in the course of providing telecommunications services (including personal particulars, location and information about a customer's use of the service) except for permitted purposes and except as otherwise authorised by law.	stored communications would provide access to the content of a communication, whereas the data retention regime under the TIA Act does not require carriers to record or store the content of communications. Concerns about the possible designation of this information were raised by stakeholders.[80] Stored communications which reveal the content and substance of an individual's communications with others may be considered to entail even greater privacy sensitivity than metadata alone. This is reflected in the TIA Act which affords stored communications greater privacy protection than metadata, by stipulating that access to the content of stored or live communications can only be obtained by law enforcement agencies with a valid warrant. The key privacy impact of sharing content and substance of communications is the detailed and personal information it would reveal about any person who is a party to the communication. Content of communications could reveal more	received from consumers, and to maintain a high standard in terms of their data security.	potential for this information to reveal very sensitive and detailed information about consumers. Unlike other datasets often considered to be highly sensitive, while consumers currently have access to some of their own communications (for example, text messages, email archives and personal cloud storage), the sharing of this information with third parties is not prevalent. While privacy impact is one of the statutory factors to be considered among others in making a designation decision, stakeholders did not identify any use cases for this type of information. Therefore, we do not consider that the benefit to consumers of sharing this information could outweigh the significant privacy risks, and we recommend that content or substance of communications be excluded from designation.

[79] In the telecommunications sector, stored communications are generally cached copies of data or files transmitted over the internet including emails. Carriers do not record and store all communications transmitted over voice telephony networks.
[80] OAIC submission, p.13; AISA submission, p.3; Finder submission, p.11.

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
	The TIA Act sets out certain exceptions to these prohibitions to permit eligible law enforcement agencies obtain warrants to intercept communications, to access stored communications and to authorise the disclosure of data to investigate a 'serious contravention of the law'.	unique and nuanced information about an individual than discrete data points from which inferences can be drawn, but from which key context may not be revealed. For example, a consumer's data may reveal they made a particular purchase but from the data alone it is unknown whether the purchase was for the consumer or a gift for someone else. Content can be much more contextual and remove the 'element of doubt' that can be associated with drawing inferences from data points.		
8	**Information about the existence of a financial hardship arrangement** Hardship policies are developed by providers to identify and assist customers experiencing financial hardship, for example, as result of a financial, health, family, or other matter. Financial hardship refers to a situation where a consumer is willing to pay a debt but does not have the financial capacity to do so	The OAIC submits that this information could be highly sensitive to individual consumers in that it could reveal insights about their financial capacity which could, for example, influence the goods and services subsequently offered to them.[81] This impact would directly affect consumers experiencing financial vulnerability, but it may have a disproportionate impact on consumers with other vulnerabilities – such as consumers with low literacy levels, the elderly, and consumers who may be impacted by family or domestic violence.	The consent rules ensure that consumers give informed and express consent to the collection and use of their data, and this includes actively selecting which data they share and for what purposes. Any sharing of information about the existence of hardship arrangements would be subject to the existing rules around consent including the requirement that this information be actively selected and the consent to share it is informed and not bundled in with consents for other, less sensitive categories or sub-categories of CDR data. The standards could ensure that information about the existence of a financial hardship arrangement could be presented as its own data cluster in the consent process.	There are existing mitigation strategies for this kind of data already in place in the CDR regime and subsequent rule and standards making processes that could address the privacy impact of sharing this information – for example, through ensuring that this information is presented as a standalone data cluster that consumers must actively select to share during the consent process, and ensuring that processes for asking for consent to collect and use this particular dataset are sufficiently transparent to enable a consumer to make an informed decision about sharing it. This will ensure that CDR consumers are given sufficient control over whether to share this information about themselves. However, there is a lack of evidence to support how including consumer information about the existence of hardship arrangements could drive consumer

[81] OAIC submission, p. 13.

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
	according to their contractual obligations.			benefit and innovation. Therefore, having weighed the privacy risk against the range of other statutory factors, we do not recommend that this information be designated. We consider this could be revisited in the future if compelling use cases emerge and appropriate mitigation strategies to address the sensitivity of this information are considered. This approach is consistent with that taken in the energy sector. While information about hardship was included in the designation instrument for the energy sector, the rules have not required it to be shared.

Part III: general privacy impacts of telecommunications designation

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
9	**The potential for sharing data from accounts with more than one user**	Many telecommunications accounts have more than one account user and the additional users (end users) of an account may not be the account holder or billing entity. For example, where multiple services used by a family are connected under one account and one adult is the account holder, or business plan arrangements where an employer is the account holder and its employees are account users. The Australian Communications and Media Authority (ACMA) and AISA have raised privacy concerns about the potential for the CDR to enable account holders to access consumer data about third party users of the account.[82] For example, if carrier location data were designated, there is concern that an account holder could share the location of a mobile service linked to their account with a third-party for the purpose of tracking the movements of an employee or family member. In the business account context, there could be privacy implications for a third-party employee if an employer is able to access information about an employee's service linked to the	The CDR rules contain mechanisms for sharing data on accounts with more than one user – including joint account holder rules, secondary user permissions (for example, secondary cardholders) and the ability for businesses to nominate representatives to manage their CDR data sharing. The rules prohibit ADRs from requesting consent to use CDR data for the purpose of identifying, compiling insights in relation to, or building a profile in relation to, any identifiable person who is not the CDR consumer making the consumer data sharing request. The rules also include provisions to prevent physical or financial harm, or abuse of consumers where necessary, including where data sharing is occurring or may occur from an account with multiple users.	The privacy impact of sharing data from accounts with more than one user depends in part on the ultimate scope of designation. Based on the recommendation, that consumer data designation would consist of information that is already available to consumers (for example, on bills), the inclusion of accounts with multiple users does not present an insurmountable privacy risk. This is because account holders are already able to access this information. Further consideration will be given at the rule-making stage to any privacy impacts for accounts with multiple-users having regard to the datasets proposed for sharing at that stage.

[82] ACMA submission, p.5; AISA submission, p. 3.

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
		business account, particularly where the employee uses a service for both business and personal use.		
10	**Cumulative privacy and security risk associated with combining datasets from multiple sectors**	AISA raises concerns that as data recipients begin to collect consumer data from multiple sectors, the privacy and security risks multiply. These include security risks associated with the creation of data 'honeypots' attractive to cyber-criminals and privacy risks associated with increasingly detailed information about individuals being brought together and analysed.[83] The OAIC also notes that combining data from different sectors means richer and more granular insights may be derived about individual CDR consumers, meaning the sensitivity of the data and the overall privacy risks for consumers may increase.[84] Consumers may be unaware of the potential for sensitive conclusions to be drawn from combining their CDR data related to several sectors for example, banking data with telecommunications data, and these risks may be exacerbated for vulnerable consumers.[85]	These risks are mitigated by the strong privacy and consumer protections in the regime. For example, robust information security requirements, safeguards around the deletion and de-identification of CDR data, requirements that restrict an ADR's use of data in accordance with a consumer's informed consent (including how long it can be used for and the purposes for which it can be used) and the principle of data minimisation.	The CDR is intended to be an economy wide reform legislative framework and as such, the CDR regime's security and privacy framework was developed to ensure the safe and secure handling of data from multiple sources and sectors. As the CDR matures and considers technological developments, additional requirements in relation to information security will be managed at the rule and standards making stages as appropriate.

[83] AISA submission, p.2.
[84] OAIC submission, p. 5.
[85] OAIC submission, p.5.

No.	Item	Privacy impact	Existing mitigation strategies	Gap analysis and recommendation regarding designation with respect to privacy
11	**Telecommunications sector specific privacy risks**	The OAIC notes that the application of the CDR to the telecommunications sector will result in increased data flows as well as handling of telecommunications data by entities that may not have previously handled this type of information. The OAIC notes this could increase the risk of unauthorised access to or disclosure of telecommunications data, for example, due to hacking, identity theft and fraud incidents, absent strong safeguards.[86] See also Item 1.	The risk of customer data being used inappropriately is mitigated by the CDR accreditation process under which third parties must meet rigorous privacy and security requirements before they can receive and use CDR data. These requirements must be maintained when a person has become accredited, and include implementing a security governance framework, maintaining a comprehensive information security capability, managing and reporting security incidents, and requirements around who has access to data within an ADR's CDR data environment. ADRs are also bound by the 13 privacy safeguards which relate to how an ADR uses and handles CDR data. A breach of the privacy and security protections in the regime can result in enforcement action being taken against the relevant ADR. Strong individual authentication requirements are also embedded in the CDR data sharing process with strong customer authentication required for data holders to authenticate CDR consumers, before they can disclose CDR data to an ADR.	Our analysis of submissions to the consultation on a potential designation of the telecommunications sector have not revealed any sector-specific privacy risks that support a conclusion that the sector not be designated for privacy reasons. As noted throughout this assessment, except for data about the content or substance of communications, the rules and standards can appropriately mitigate the privacy impact of sharing data that could be included under any telecommunications designation.

[86] OAIC submission, p. 6.

Grant Thornton

Attachment B

Regulatory Impact of the CDR in Telecommunications

Commonwealth Department of the Treasury

November 2021

[redacted]
Acting Director
Sectoral Assessments
Consumer Data Right Division

3 November 2021

Grant Thornton
Collins Square, Tower 5
727 Collins St,
Melbourne VIC 3008

www.grantthornton.com.au

Dear [redacted]

Thank you for the opportunity to assist the Department of the Treasury in conducting a review of the impacts and potential costings to the Telecommunications sector being included in the Consumer Data Right (CDR) program. This report contains the results of our engagement including details on our scope, approach and key findings. Where feasible, we would encourage readers to review our report in its entirety to fully understand our findings in the appropriate context.

Forms of report

For your convenience, this report may be made available to you in electronic as well as hard copy format. Multiple copies and versions of this report may therefore exist in different media and in the case of any discrepancy the final signed copy should be regarded as definitive.

Location and period of fieldwork

This report is based on work completed during the period 13 October 2021 to 27 October 2021. Fieldwork was performed remotely with various stakeholders (refer to Appendix 1).

Confidentiality

This report has been prepared for Treasury to be published and should not be quoted in whole or in part without our prior written consent. We acknowledge that this report has been prepared to assist in the broader sectoral assessment for telecommunications and will be referred to in the Telecommunications sectoral assessment - final report (November 2021).

No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other party. The report is issued on the understanding that the contacts at the Treasury have drawn our attention to all matters, financial or otherwise, of which they are aware which may have an impact on our report up to the date of signature of this report. Additionally, we have no responsibility to update this report for events and circumstances occurring after this date.

Limitation of liability

We draw your attention to the limitation of liability clauses in our engagement letter which is included in your statement of work.

Scope of work and limitations

The scope of our work has been limited both in terms of the areas of the program and entities which we have considered and the extent to which we have considered them. There may be matters, other than those noted in this report, which might be relevant in the context of the CDR program, which a wider scope review might uncover.

To facilitate stakeholder discussions and guide the cost impact analysis, the following designated classes of data were deemed in scope:

- Product reference data:
  - Retail product information
- Consumer data
  - Retail product information as it relates to a particular product used by a consumer
  - Information about a customer or user of a product
  - Information about the use of a product

The conclusions and estimates stated in this report may be invalidated by additional information not made available at the time of our work.

Contacts

If there are any matters upon which you require clarification or further information please contact Daniel Farthing, Engagement Director, at [redacted] or Matt Green, Engagement Partner, at [redacted].

It has been our pleasure working with you, your team and the industry contacts throughout this review. We are excited about the opportunities that come with the Consumer Data Right more broadly and are thankful for this opportunity to be involved in the program.

We look forward to the opportunity to work with Treasury again in the future.

Matthew Green
Partner
Grant Thornton Australia Limited

Contents.

Authors: Mathew Green – Partner, Consulting

Daniel Farthing – Director, Consulting

Kate Wilkie – Manager, Consulting

Review date: 13 October 2021 to 29 October 2021

To: The Treasury

Cc: [redacted], Acting Director, Consumer Data Right Division

[redacted], Analyst, Consumer Data Right Division

Executive Summary

Executive Summary

Scope

This review focussed on the regulatory impact of compliance to the Consumer Data Right (CDR) for data holders and data recipients as part of a proposed designation of the Telecommunications sector.

Grant Thornton was engaged by Treasury (Official Order CO3350 signed 12 October 2021) to conduct analysis of the estimated regulatory impact for data holders should the telecommunications sector be designated for rollout of the CDR. To a lesser extent, we also considered the regulatory impact for data recipients that will be seeking to ingest telecommunications data.

This engagement included the following aspects :

- Consulting with stakeholders as agreed with Treasury, including:
  - Retail service providers that may be designated as Data Holders (large, mid-tier, small)
  - Existing vendors offering CDR software solutions to data holders in the Banking sector and/or the Energy sector
- Analysing estimated costings for Data Holders to comply with CDR requirements, including establishment and ongoing costs.
- Whether there will be incremental costs for Accredited Data Recipients (ADRs) to participate in the telecommunications CDR.
- Provision of a written report that summarises our approach and provides findings related to the above items.

Approach

Grant Thornton participated in **8** stakeholder consultations with representative organisations from across the Telecommunications sector, including data holders and potential service providers to understand the relative regulatory impact of designating the telecommunications sector for CDR. The list of organisations consulted is in **Appendix 1**.

Stakeholder consultations were conducted virtually over a 2-week period, from 18 October to 27 October 2021.

The subject matter covered with Data holders during those meetings included:

- Each organisation's understanding of the CDR
- Current state of proposed data sets / infrastructure
- Experience with similar regulatory initiatives (eg data retention)
- Any complexities that are specific or unique to their organisation
- Potential suggestions to mitigate or reduce the regulatory impact

The subject matter covered with current and potential outsource service providers during those meetings included:

- Potential to provide an 'out of box' solution for Telecommunication data holders
- Experiences working with data holders to date

Findings

Based on consultations with selected stakeholders, and the information provided, estimated minimum regulatory impacts (in terms of costs) have been developed for an indicative small and an indicative large data holder based on a proposed 'low regulatory impact' regime (refer to slide 8 for more details):

- Small Telco Year 1 (Build and run): **$340,000**
- Small Telco Year 2 (run): $**160,000**
- Large Telco Year 1 (Build): **$4,300,000**
- Large Telco Year 2 (run): **1,280,000**

These estimated costings are highly caveated given they are based on consultations with stakeholders before the development of detailed rules and standards that will support any future implementation of the CDR in telco. At this point in the Sectoral Assessment process, telco data holders were unable to provide specific data related to the potential cost implications of designation. More specific cost estimates, however, were provided by the potential outsource service providers to the sector based on their experience gained in other sectors.

As part of the consultation process, a number of areas were consistently raised as key items that would greatly influence whether the implementation of the CDR in telco would result in a lower or higher regulatory impact. These items included the timeline for implementation as well as the exact scope of the datasets and customer types and products that would be subject to the CDR (refer to slide 7 for a list of these key items). The Regulatory Impact Analysis section of this report provides further information on some of these key considerations that are likely to be decided in the Rule-making process as well as potential mitigating activities which may reduce the regulatory impact.

Cost estimates provided by Stakeholders

Reference point	Estimated / Referenced Cost[1]	Estimate Provided By	What is included	Why this estimate may not be accurate
Subscription Product Reference Data (PRD) & Consumer Reference Data (CRD) Estimates				
Subscription service to provision PRD	**$30K** (annually)	Third-party data aggregator	• Publicly available Product data which has no privacy or security requirements	• Does not include Build/Run cost to Telcos to provision data to the data aggregator
Subscription service to provision CRD	**$180K - $240K** (annually)	Third-party data aggregator	• Industry compliant APIs to provision CRD • Authentication • Consent	• Does not include Build/Run cost to Telcos to provision data to the data aggregator
Subscription service to provision PRD & CRD	**$140K** (annually)	Third-party data aggregator	• Industry compliant APIs to provision PRD/CRD • Authentication • Consent	• Does not include Build/Run cost to Telcos to provision data to the data aggregator • Actual costs will be fixed + variable for each data holder
Estimates of Build / Run Costs for Telcos				
Build costs for Telco to provision CDR data	**$200K+** – Small to midsize **$3M - $4M** – Large Telco	Third-party data aggregator	Costs to develop back-end systems capable of provisioning CDR data (both PRD & CRD)	• Does not include scoping/discovery costs • Does not include infrastructure upgrade costs (digital transformation) • Does not account for significant variation in different organisations' ability to leverage existing technology for the CDR
Build costs for Telco to provision CDR data	**Mid $10Ms**	Major telco provider	Costs to develop back-end systems capable of provisioning CDR data (both PRD & CRD)	• The telco provider did not have sufficient time to consider the proposed datasets • This estimate was not based upon a 'low regulatory impact' regime
Run costs for Telco to provision CDR data	**$20K - $30K** (annually) Small to midsize	Third-party data aggregator	Ongoing operational costs to Telcos to provision data to CDR	• Does not account for significant variation in different organisations' ability to leverage existing technology for the CDR
Other Cost Estimates Flagged During Stakeholder Consultations (Various)				
Estimated cost to telco industry of data retention regulation	**$240M** (all in cost over 5 years)	Major telco provider / ACMA[2]	All-in costs for compliance	• Not a direct comparison to the CDR • The cost included implementation and run costs over a 5 year period • Primary driver of cost (increased technology infrastructure for the increased storage of data) is not fully applicable to the CDR
Build costs for Telco to provision **enterprise customer** data to CDR	**2X or 3X** the cost of the CDR for non-enterprise customers	Major telco provider	All-in costs for compliance	• The estimate provided is likely a minimum cost given the nuances and customised nature of services provided to these customers and the internal systems used in the management of these customers.

1 All figures have been provided as estimates only with minimal consideration for the specific circumstances of any individual data holder
2 https://www.acma.gov.au/sites/default/files/2020-12/Telecommunications-law-enforcement-and-national-security-obligations-2019-20.pdf

Key rules and implementation decisions will significantly impact the regulatory impact to data holders

Areas raised by telco stakeholders	Considerations that will increase or reduce Regulatory Impact	
	Lower Regulatory Impact (Lower Cost to Data Holders)	**Higher Regulatory Impact** (Higher Cost to Data Holders)
1. Industry readiness	• Industry is given a long lead time from designation • Consultation forums are established with key stakeholders • CDR rules are harmonised with existing regulations	• Implementation timelines are constricted and applied with minimal consultation • CDR rules do not consider or contradict existing regulatory frameworks
2. Current technical landscape	• CDR implementation timeline and approach considers existing digital transformation programs • Existing protocols for authentication are leveraged	• Data holders are required to implement CDR solutions to legacy technology
3. Scope of datasets	• Datasets are consistent with those used in this consultation and similar to the datasets already provisioned to consumers via digital channels • Additional datasets are considered in a phased and consultative approach	• Datasets are extended beyond those currently and consistently provided to consumers via existing channels (eg performance and location data)
4. Enterprise and complex customers	• The ACMA definition (or potentially a more restrictive definition) of enterprise customers is adopted • Enterprise customers are excluded from the CDR	• Inclusion of datasets and products relating to enterprise or more complex customers
5. Data latency and history	• Data available to consumers is historic in nature (eg as of previous billing cycle) • Historic data requirement is for a shorter time period (eg 6 months) • Maintain consistency with existing latency updates in digital channels? (eg daily updates in a mobile app)	• Data available to consumers is real-time • Historic data requirement is for a longer period of time (eg over 1 year)
6. Phasing of rollout	• Implementation is phased either by size of data holder, customer type, data set (eg product data as opposed to consumer data) or product type (eg pre-paid mobile as opposed to broadband)	• All CDR participants and data are required to be live at the same time
7. Usage of intermediaries	• Data holders use intermediaries (eg data aggregators) to assist in the provision of the CDR data, where the provisioning of data to intermediaries is straightforward.	• Intermediaries are not able to provide a solution for data holders, or the provisioning of data to intermediaries is complex and requires significant internal technical solution builds.
8. Scope of products	• De minimis products (for example $5 plan for calls and texts) are excluded from the CDR • Legacy and grandfathered products are excluded from the CDR	• Certain products, specifically those where consumer information is not currently made available via digital channels, are included in the CDR

Minimum Cost Estimate for Indicative Data Holders in a Low Regulatory Impact Regime

Scope	Complexity of Data Holder	
	Small Telco	Large Telco
Implementation Costs		
Discovery Cost	$60,000	$600,000
Product Reference Data Solution	$30,000	$300,000
Consumer Reference Data Solution	$170,000	$3,400,000
Total Build Costs	**$260,000**	**$4,300,000**
Ongoing Annual Costs	PRD / CRD 3rd party subscriptions	PRD 3rd party subscription
Product Reference Data Solution	$20,000	$200,000
Consumer Reference Data Solution	$120,000	$680,000
Run costs	$20,000	$400,000
Total Ongoing Costs	**$160,000**	**$1,280,000**
Example Costs By Year	6-month implementation timeline	12-month implementation time
Year 1	**$340,000**	**$4,300,000**
Year 2 and Beyond	**$160,000**	**$1,280,000**

Caveats and Assumptions

- The estimates provided are presented as minimum amounts that it might cost a data holder to become compliant and are not intended to represent the most complex implementations within each cohort.
- The estimated costings assume a regulatory impact that aligns with the “Lower Regulatory Impact” section on the previous slide.
- Estimated costings do not include costs associated with required upgrades to legacy infrastructure (“digital transformation”).
- Costings are based on estimated ‘all-in’ costs provided via formal stakeholder consultations as well informal feedback from experiences in other sectors.
- At the time of this exercise, estimates for time required to complete individual activities were not available meaning a ‘bottom-up’ cost estimate could not be prepared.
- The estimated costing assumes that third-party technology solutions (eg data aggregators) are available in the market and utilised as noted.

Regulatory Impact Analysis

Analysis Approach and High Level findings

Approach

In order to gain an improved understanding of the potential regulatory impact of designating telco for CDR, we participated in consultations with a range of stakeholders comprised of large and mid-sized telcos along with potential outsource service providers (OSPs). Given obtaining detailed costings is not a straightforward exercise, we also asked stakeholders about the implementation areas that were likely to be the most difficult / complex. As a result of these efforts, we obtained some high level costing estimates along with key areas that will dictate the magnitude of the regulatory impact in telco.

The following steps were taken:

- Documentation review of previously supplied submissions provided by the sector.
- Desktop review of costing impacts to the Banking and Energy Sectors.
- Stakeholder consultations with representative organisations from across the sector, including data holders and OSPs.
- Summarise the key challenges and opportunities impacting the cost of CDR compliance.
- Interrogate comparative costings and develop a potential cost estimate for indicative data holders.

Consultation Undertaken

A representational stakeholder group from the sector was invited to provide insights into the impact of CDR compliance and discuss opportunities to enable a robust solution.

The focus areas covered with Data holders during those meetings were:

- Organisation's understanding of CDR requirements
- Current state of proposed data sets / infrastructure
- Experience with similar regulatory initiatives (eg data retention)
- Potential suggestions to mitigate or reduce the regulatory impact

The focus areas covered with current and potential data recipients during those meetings were:

- Potential to provide an 'out of box' solution for Telecommunication data holders
- Experiences working with data holders to date
- Program design

Documentation Review

Documentation provided by the Department of Treasury was reviewed to give context to and inform the discussions held. This included Telecommunications Sectorial Assessment - Consultation Paper submissions provided back to the Department of Treasury.

High Level Results

As a result of the consultations undertaken and the documentation reviewed, 8 key areas were identified as having the greatest impact to the sector. This was in regard to both cost and time impacts.

Regulatory Impact Drivers

- Industry readiness
- Current technical infrastructure
- Scope of datasets
- Enterprise customers
- Data latency
- Phasing of rollout
- Usage of intermediaries
- Scope of products

1. Industry Readiness

Key Takeaways

- Telco is less familiar with the CDR and consider themselves to be less ready than Banking or Energy
- The number of data holders in telco is larger than Banking or Energy with many smaller and niche players
- Rapid introduction of new products to market
- There are more products and more variations within products than Energy

Telco is a diverse sector where familiarity with the CDR is currently low

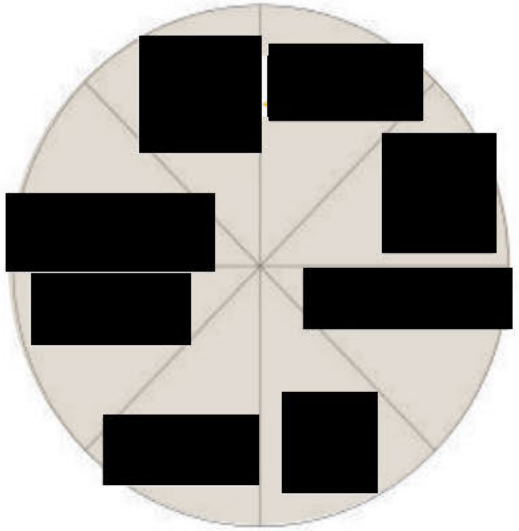
Within the Telecommunications sector, there is currently a relatively low level of understanding of the CDR and the efforts required to provide compliant solutions. This is due in part to the lack of an industry driver for such a legislative change (unlike the 'Review into Open Banking in Australia' report for Banking and the 'Open Consumer Energy Data' report for Energy) and minimal reference points available internationally.

When compared specifically to Banking, the telco sector has a lower level of entry regulation to become a retail provider, which has led to a wide and diverse number of organisations operating within the market. Similar to Energy, outside of the top and mid-tier providers, there are a large number of quite small retailers for which compliance with the CDR may present a significant challenge.

The market has also experienced significant consolidation within the last decade which has led to an amalgamation of legacy products ('grandfathered' products) that are being maintained by a small number of large players. The majority of the larger providers also have extensive white label offerings.

In comparison to the Banking and Energy sectors, the telco sector has a wider and less standardised range of products. Margins are constantly under pressure from the introduction of new products to the market. The sector is transitioning from less consumption-based products (eg a certain number of calling minutes or amount of data) to more 'unlimited' products where price and performance are the key differentiators.

Impact raised across consultations



Consultations raised 'Industry Readiness' as a key concern to them:

8 out of 8

Options to Reduce Regulatory Impact

- Provide longer lead times and/or a phased approach to implementation to allow organisations the bandwidth to understand and implement changes
- Provide forums for consultation and collaboration
- Where possible, harmonise the CDR definitions and protocols with existing regulations in the sector
- Consider exemptions for providers that have a smaller number of retail customers

2. Current Technical Landscape

Key Takeaways

- Less centralisation of data sets as some technology infrastructure is product specific (no core Banking equivalent)
- Many organisations are transitioning legacy technology to digital platforms
- High level of complexity based on product offerings and legacy systems
- Most telcos consulted have existing mechanisms for consent, authentication and sharing data via APIs

Disparate systems and legacy technologies will require upgrades to implement the CDR

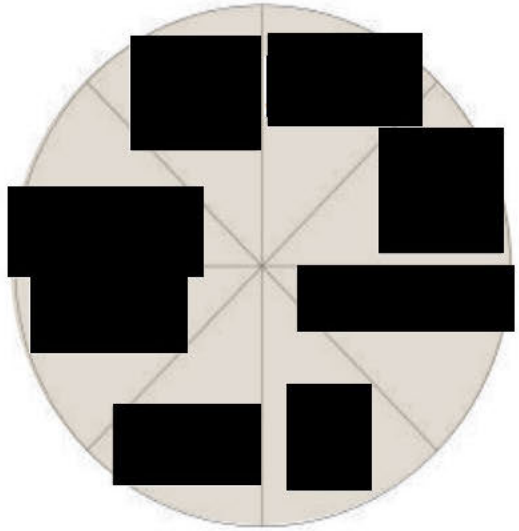
The technology landscape within the telecommunications sector is reflective of the change and innovation of the sector itself, particular in the accelerated rate of change seen in the sector in recent years. This is especially apparent at the larger providers who have grown through mergers and acquisitions.

Systems within the telco sector are not are often aligned around a particular customer cohort or product type. There is no core system used across the board. Within the larger providers, there may be multiple systems holding similar datasets or even multiple systems with independent records related to a single customer. This is particularly the case with reference to legacy customers and grandfathered products. There is a strong reluctance from stakeholders to implement a CDR solution for such legacy systems which are due to be replaced under current digital transformation programs of work.

With the exception of one large retail provider (who already has a unified digitalised system infrastructure), multi-year programs of work are underway to migrate to digital platforms. The initial focus of these projects is upgrading the retail systems which have less complexity and less reliance on legacy systems than the commercial/enterprise systems.

Pleasingly, most stakeholders consulted already have mechanisms in place related providing/tracking consent, authentication of customers (eg one-time pins) and sharing of data via APIs. Though these areas have not been tailored for the CDR, they should serve as reasonable basis for implementing a CDR solution.

Impact raised across consultations



Consultations raised 'Current Technical Landscape' as a key concern to them:

8 out of 8

Options to Reduce Regulatory Impact

- The CDR implementation timeline and approach considers existing digital transformation programs
- Where possible, harmonise the CDR definitions and protocols with existing regulations in the sector

3. Scope of Datasets

Key Takeaways

- Earlier consultation included a broader range of datasets than the proposed designation scope, including location and broadband speed data. Such datasets would increase complexity as these are not currently provided via digital channels
- Decreasing utility of 'usage' as a dataset
- Importance of agreed data set definitions – particularly in relation to product terms between providers

Stakeholders were receptive to the datasets proposed in consultations (ref Appendix 2)

The final designation of the datasets for the Telecommunication sector will have a significant impact on the cost and timeframe for providers to achieve compliance. The datasets initially proposed in the consultation paper were quite broad in scope and covered data related to customers, products, product usage and quality measures

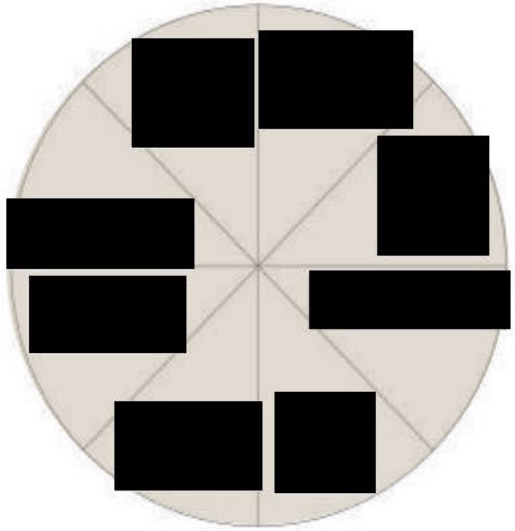
There was strong and consistent resistance in both the written submissions reviewed and in the stakeholder consultations held that datasets related to performance and quality (such as broadband speed and mobile coverage) and location went further than the definition of 'consumer data' in other sectors and these datasets would be quite costly to implement in the near-term. Additionally, concerns around privacy were raised with regards to the location dataset. As these datasets were excluded from the proposed scope in the stakeholder consultations (which broadly aligns with the proposed scope in the final report), stakeholders were generally positive about the remaining scope.

As highlighted in the Industry Readiness slide, telco products are changing from more consumption based products (eg a certain number of calling minutes or amount of data) to more 'unlimited' products where price and performance are the key differentiators. Additionally, usage related to calls and SMS messages is becoming less relevant as many over-the-top (OTT) applications such as iMessage, WhatsApp and Facetime are increasingly popular and provide similar functionality. As a result, datasets related to 'usage', may become less relevant to consumers over time.

With regards to product reference data, there will be some effort to transition Critical Information Summaries (which are often stored in .pdf files) to digital formats – though this challenge should not require significant cost to achieve.

Once the final classes of data are determined for designation, there was consistent feedback regarding the need to agree on the specific datasets for sharing (which would occur at the rule-making stage) particularly in relation to product terminology across providers, but also considering alignment to the definitions under existing regulations.

Impact raised across consultations



Consultations raised 'Scope of Datasets' as a key concern to them:

8 out of 8

Options to Reduce Regulatory Impact

- Datasets are consistent with those used in this consultation and similar to the datasets already provisioned to consumers via digital channels
- Additional datasets are considered in a phased and consultative approach

4. Enterprise and Complex Customers

Key Takeaways

- Enterprise customers generally are able to negotiate terms meaning there is little standardisation of products and contracts
- Lower regulation of Enterprise Customers including lack of industry requirements for consent, authentication, privacy
- Lack of consistent definition across stakeholders
- Segregated technology infrastructure

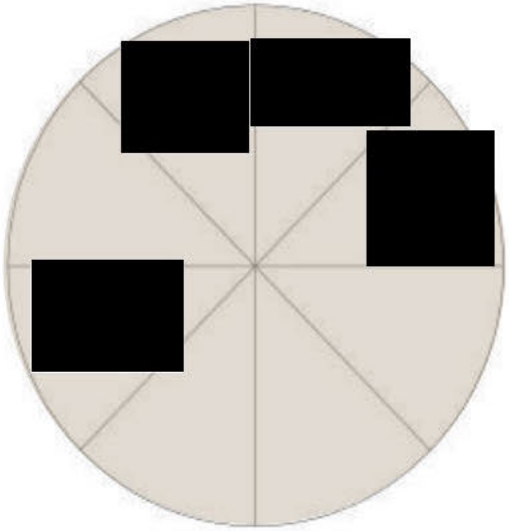
Enterprise customers add significant complexity to implementing the CDR in telco

In each consultation with data holders, the challenges related to enterprise customers were a consistent theme when discussing the complexities of implementing the CDR. Even the definition of enterprise customer involves complexity – with some deferring to the ACMA definition of an annual spend of $40,000+ while others highlighted that complex commercial customers exist below this threshold.

At core of the issue is that enterprise customers are treated differently in the sector than retail customers and sole proprietorships. Enterprise customers are characterised by the ability to negotiate terms and products to suit their needs, do not attract the same level of regulation (eg consent and privacy rules) and, generally, are supported by segregated (and often legacy) enterprise systems. It was also consistently raised that enterprise customers are less likely to derive benefits from the CDR as their needs are already understood and tailored during the contracting phase.

Due to the lack of standardisation in the provision of services in this segment of the industry, the impact of including enterprise customers within the scope of the CDR may result in an exponential increase in the complexity, cost and timeframe required for the larger telecommunications providers to comply with the CDR requirements. One stakeholder flagged that the likely impact is potentially twice to triple the cost of implementing the CDR for retail customers – and, based on the complexity involved, even this number might be conservative.

Impact raised across consultations



Consultations raised 'Enterprise and Complex Customers' as a key concern to them:

4 out of 8

Options to Reduce Regulatory Impact

- The ACMA definition (or potentially a more restrictive definition) of enterprise customers is adopted
- Enterprise customers are excluded from the CDR

5. Data Latency and History

Key Takeaways

- Real-time data is less common in the telco sector compared to Banking
- Real-time data is primarily related to usage and this may become less relevant over time (refer to 3. Scope of Datasets)
- Provision of aged data ('Data History') will also present a challenge as some providers do not maintain data in a retrievable format for longer than 6 months
- Existing regulation requires customer notification of 'usage' based products which are set at specific limits

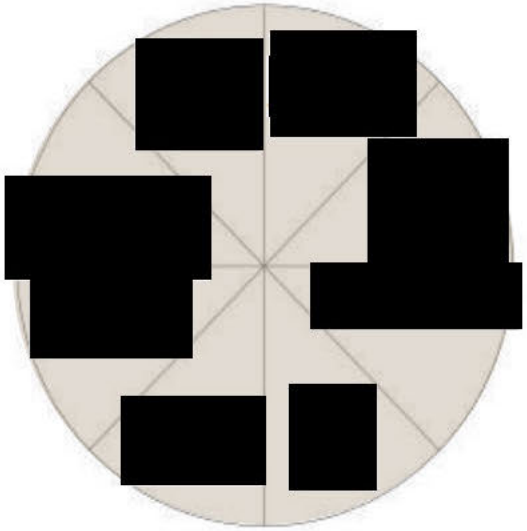
Current data latency and history practices in telco are at odds with the CDR implementation in other sectors

Data latency was raised by stakeholders due to the potential difference to latency in the telecommunications sector compared to the Banking sector, where consumers are often able to see real-time updates in their mobile apps. Some larger retailers have existing mechanisms to provide usage data on a real-time basis, however, other providers intentionally limit their product and services such that real-time data is not necessary. With regards to all other types of data, industry practice is for data to be provided in alignment with billing cycles, which are commonly a monthly process.

Consumption-based products fall under existing regulations which require alerts to be provided to customers at specific limits (eg 50%, 75%). The functionality which enables this is either built into the corresponding product system or a specific 'add-on' has been created to enable this function. It was noted that handsets were now able to provide a wide range of 'real-time' data relating to the data or application usage. The evolution of product offerings (i.e.: unlimited calls and texts) has further reduced the relevance of the provision of this data in real time to the customer.

Beyond latency, the ability to provision historic data was of particular interest for one large telco. It was communicated that it is currently common practice to only maintain historic data in a readily retrievable format for 3 to 6 months – which would be a much shorter time than Banking. After 3 to 6 months, the data is archived and retrievable in the form of a historic statement. If the CDR requirements include provisioning of data for a historic period greater than 3 to 6 months, this may require significant investment and increase in storage across the industry.

Impact raised across consultations



Consultations raised 'Data Latency and History' as a key concern to them:

8 out of 8

Options to Reduce Regulatory Impact

- Data available via the CDR is aligned with the consumer's billing cycle (eg monthly)
- Historic data requirement is for a shorter time period (eg 3 - 6 months)

6. Phasing of Rollout

Key Takeaways

- A phased rollout may decrease regulatory impact, increase initial compliance and negate the requirement to 'build it twice'
- Phasing could be done around size of retailer, datasets, products or customers

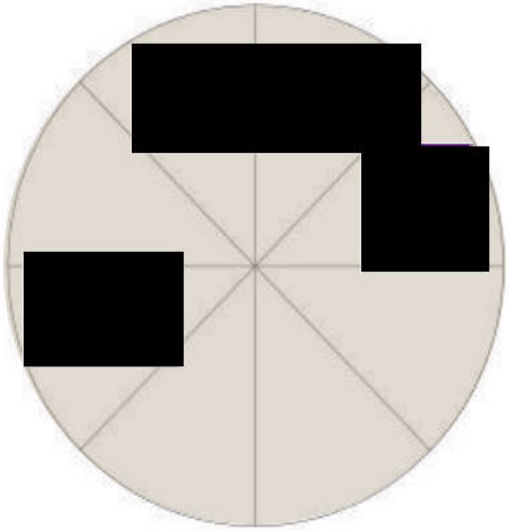
Phasing the rollout of the CDR in telco will likely decrease the regulatory impact of designation

The adoption of a phased rollout in telco, similar to that which has occurred in Banking, was widely supported in stakeholder consultations. A phased rollout for compliance would likely have a direct impact on all providers within the sector.

As highlighted in previous slides, many larger telcos are currently maintaining legacy products supported by the disparate legacy systems. There was significant resistance in applying the CDR to these legacy products. By introducing the CDR in a phased approach, however, with sufficient time to consider and implement each scope, it potentially provides the time for necessary uplift and transformations to occur. As a result, the phased approach to implementation increases the likelihood of compliance by each data holder.

Similar to Banking, an approach that first requires product reference data (PRD) and then shifts to consumer data (CRD) may also be prudent as PRD is likely to be simpler to provision and allows organisations some time to become familiar with the CDR program.

Impact raised across consultations



Consultations raised 'Phasing of Rollout' as a key concern to them:

4 out of 8

Options to Reduce Regulatory Impact

- Implementation is phased either by size of data holder, customer type, data set (eg product data as opposed to consumer data), product type (eg pre-paid mobile as opposed to broadband) or customers

7. Usage of Intermediaries

Key Takeaways

- Outsource service providers (OSPs) who are able to help data holders to develop and implement compliant systems decrease the regulatory impact

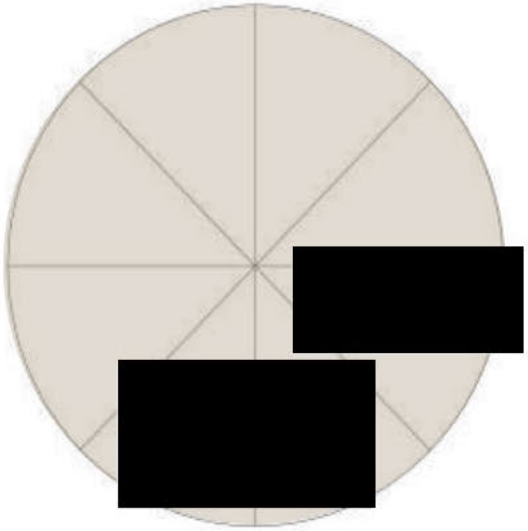
Intermediaries present an opportunity to reduce regulatory impact

Whilst significant costs are involved in developing and upgrading technology systems to be able to provision required CDR data, there are also costs in the development of the product data solution, APIs, authentication mechanisms and consent management dashboards that are required to comply with the regulations. As the latter items are more able to be standardised across the sector, these items are attractive to OSPs who wish to enter the market to assist data holders to become compliant.

During the stakeholder consultations, it was flagged that Treasury could facilitate OSP involvement by ensuring that the above listed items are as consistent as possible between previous sectors (Banking and Energy) and telco. Maintaining consistency decreases the upfront cost required to adapt existing solutions to telco and improves the cost/benefit analysis of targeting the sector.

In addition to the above, one stakeholder raised the concern that the apportionment of data holder liability and cost of cyber insurance were key barriers to entry for OSPs. In the case of the former, the regulatory liability remains with the data holder even though there may be outages in an OSPs system. In the latter, this is a natural result of an OSP having access to significant consumer information from data holders. For both items, no recommended solutions or mitigating actions were identified as part of the consultation process and, as such, they are presented here without further comment.

Impact raised across consultations



Consultations raised 'Usage of Intermediaries' as a key concern to them:

3 out of 8

Options to Reduce Regulatory Impact

- Where possible, maintain consistency (with previous sectors) in the protocols and standards for authentication, consent and relevant APIs
- If required, clarify that intermediaries are not forbidden from assisting data holders

8. Scope of Products

Key Takeaways

- The telco industry has experienced significant change and consolidation meaning a large number of legacy and grandfathered products are still in use today
- There are products currently available in the market where information is not provided to customers via digital channels
- Some very low cost products may not be viable if CDR is required

Legacy and low cost products present unique challenges for CDR compliance

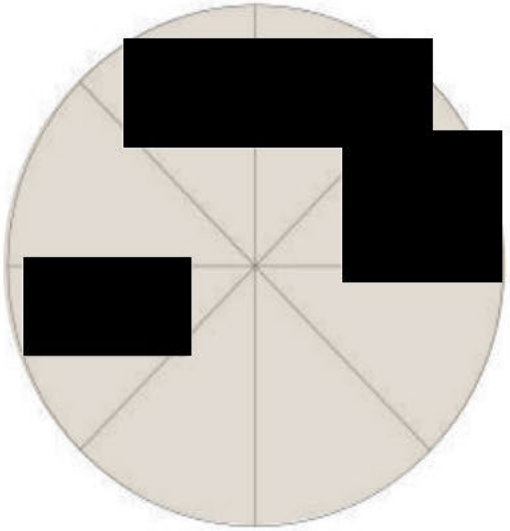
Four of the five data holders consulted in this review highlighted that they support a diverse range of products including many that have been acquired via acquisitions/mergers over the last decade. Whilst it was a common thread that each organisation had plans to migrate customers away from these legacy products over time, it was also highlighted that creating compliant solutions for these legacy products would require a high cost for low benefit (currently and into the future). Despite this, we also considered that some of the consumers on legacy products might be well suited to take advantage of the benefits afforded by the CDR.

In addition, one stakeholder highlighted the importance of being able to offer low-cost products to certain segments of the market and being able to temporarily lower costs in the case of a financial hardship. In both circumstances, the requirement to support these arrangements with CDR compliant solutions will test the viability of such products and potentially require costs to be passed to at-risk consumers.

Finally, one stakeholder consulted noted that they do not provide information via digital channels to any of their customers. For this data holder preparing a CDR compliant solution is likely to be a much harder task than for more digitally focussed providers.

The mitigating option available regarding these products is to consider whether certain products might be excluded from the scope of the CDR in the rule-making phase. If this approach is considered, we would recommend detailed analysis to ensure that competition is maintained and consumers benefits are not unduly sacrificed.

Impact raised across consultations



Consultations raised 'Scope of Products' as a key concern to them:

4 out of 8

Options to Reduce Regulatory Impact

- Consider whether particular products should be excluded from data sharing, or subject to delayed commencement for data sharing, at the rule-making stage

Appendix

Appendix 1
Consultations and Documentation Reviewed

Organisation	Name and Position
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Documentation	Author
Open Consumer Energy Data	HoustonKemp Economists
Telecommunications Sectorial Assessment - Consultation Paper	Department of Treasury
Telecommunications Sectorial Assessment - Consultation Paper submissions	• ACCAN • ACCC • ACMA • AGL • AISA • ASBFEO • Communications Alliance • Energy Queensland • Finder • illion • Internet Association of Australia • NBN Co. • OAIC • Optus • Origin Energy • Telstra • TIO • [redacted]
Various meeting and documentation summary	Department of Treasury

Appendix 2
Datasets provided for stakeholder consultation

Scope

Any designation of the telecommunications sector would involve designation of classes of information held by specified class of data holders, with the specific datasets required to be shared determined at the rule-making stage. To facilitate the stakeholder discussions and the cost impact analysis, the below table indicates the proposed scope for designated classes of data currently being considered by Treasury and related examples of datasets that could be mandated for data sharing at the rule-making stage. This scope is similar to the proposed scope in the final report, although there may be some discrepancies as this was used to facilitate the stakeholder discussions prior to finalisation of the report.

Data Type	Product Reference Data	Consumer Data	Consumer Data	Consumer Data
Class of information	Retail product information	Retail product information (as above) as it relates to a particular product used by a consumer	Information about a customer or user of a product	Information about use of a product
Scope of class	Information about products including information that: • identifies or describes a product • is about the price of a product • is about a feature or benefit of a product • is about the availability of services for disabled customers of such products (e.g., priority assistance)	Information as listed for retail product information, as it relates to a specific product that a consumer uses.	Information that identifies a customer or a user, including: • Information about a person who has or is being supplied, or has or is using, a telecommunications service (including, for example, information that identifies the user and the contact details of the user) • Information that person provided to the supplier of the service (or another person on behalf of the supplier) at the time of acquiring the service, or has provided while using the service	Information about use of a product by a customer or user typically included on a telecommunications bill, including: • Payment information, arrangements for payments, breakdowns of amounts charged such as fees, quantities of data consumed (for mobile and broadband services), and discounts applied. • Information about communications made by a customer or user in connection with the product
Example scope of required datasets in CDR rules	Publicly available product information including the information that would be contained in a Critical Information Summary or Facts Sheet, such as: • name of product • description of product • price (minimum and maximum) • fees or charges (including early termination fees) • associated features and benefits including discounts and bundles • download quantities • included calls and texts • contract term • other terms and conditions	Information as listed for retail product information. For example, if a consumer uses a product and is on a price that differs from the advertised price of a product, this could be shared as consumer (product specific) data. Similarly, this mechanism could be used to share product data for a product that is no longer publicly available (but is used by the consumer).	If the person is an individual: • Name • Physical address • Email address • Telephone number Under the current CDR rules, date of birth is not included. If the person is a business: • Business name • Physical address • ABN/ACN	Basic account and billing information, including: • Account number • Account name • Billing period • Date of bill issue • Total amount payable • Any fees, charges, or discounts • Details of usage consumption • Information about payment made in relation to bills including the date and time of payment, amount paid, and payment method

Grant Thornton

An instinct for growth™