Australian Government
Office of the Australian Information Commissioner

Our reference: D2021/012902

Ms Kate O'Rourke
First Assistant Secretary, Consumer Data Right Division
The Treasury
Langton Crescent
PARKES ACT 2600

By email: [redacted]

Re: Consumer Data Right Telecommunications Sectoral Assessment Consultation

Dear Ms O'Rourke,

Thank you for consulting me as Australian Information Commissioner on the sectoral assessment the Government is conducting of the telecommunications sector under the Consumer Data Right (CDR) framework.

I understand this consultation is occurring under section 56AE(1)(c)(ii) of the *Competition and Consumer Act 2010* (Competition and Consumer Act), as part of the Secretary's analysis, consultation and report about an instrument proposing to designate a sector. Before any instrument is made, I understand I will be consulted again under sections 56AD(3)/56AF, at which time I will be required to analyse the likely effect of making the instrument on the privacy or confidentiality of consumers' information, and report to the Minister about that analysis.

For the purposes of section 56AE(1)(c)(ii), I have considered matters relevant to the privacy or confidentiality of consumers' information as outlined in the CDR Sectoral Assessment Telecommunications Consultation Paper (the paper).

By way of general comment, and as set out further below, I note that customer information handled by telecommunications providers is inherently sensitive. In formulating my preliminary recommendations, I have taken into account whether, on the basis of the information available at this time, including certain matters in any designation instrument would be reasonable, necessary and proportionate, considering the adverse effect any such actions may have on the privacy of

individuals and whether these could be minimised to an appropriate extent.[1] I also make the general observation that further detail and clarity on the proposed datasets will need to be provided as part of the formal sector assessment report (required to be published under section 56AE), to assist me in considering the privacy impacts more fulsomely as part of my analysis and reporting obligations in section 56AF.

My comments are set out in detail below, and address the following consultation questions from a privacy perspective:

- Consultation question 11, regarding privacy issues that should be taken into account when considering the application of the CDR to the telecommunications sector
- Consultation question 4, regarding classes of data for the telecommunications sector
- Consultation question 15, regarding the ways in which the extension of CDR should take into account existing regulation in the telecommunications sector
- Consultation questions 1 and 6, regarding the boundaries of 'telecommunications data' and the 'telecommunications sector', and
- Consultation question 13, regarding the proposed data sharing model.

Recommendations

I make the following preliminary recommendations for your consideration:

1. That the privacy impact assessment explore sector-specific security risks, including by considering any feedback received from industry.
2. That location data, 'metadata' and information protected by Part 13 of the *Telecommunications Act 1997* (Telecommunications Act) be expressly excluded from the definition of CDR data in the designation instrument.
3. That a cautious approach be adopted when considering whether to designate information about financial hardship and other concessional arrangements. Our

[1] See s 28A(2)(a) of the *Privacy Act 1988* (Privacy Act), which outlines the 'monitoring related functions' of the Commissioner including in relation to the examination of proposed enactments. See also the objects of the Privacy Act in s 2A.

preference at this stage would be for such information not to be designated as CDR data.

4. That the privacy impact assessment explore the privacy issues associated with designating financial hardship/concessional information, including any impacts on vulnerable consumers.

5. That for the purposes of sectoral designation, the telecommunications sector be understood to encompass traditional telecommunication services only, and not complementary and related services.

Please advise if you would like to discuss any aspect of this letter. For your staff the contact officers for these comments are Stephanie Otorepec and Zoe Fitzell, Directors, Regulation & Strategy Branch, who can be contacted on [redacted]

I look forward to considering these matters further as part of my analysis and reporting obligations under section 56AF, and more generally to continuing our work on the CDR, to ensure that the expansion of the CDR across the economy is underpinned by strong privacy and security protections.

Yours sincerely,

[redacted]

Angelene Falk
Australian Information Commissioner
Privacy Commissioner

13 January 2022

OAIC comments on the CDR Sectoral Assessment Telecommunications Consultation Paper

Privacy issues that should be taken into account when considering the application of the CDR to the telecommunications sector (re: Consultation Question 11)

By way of general comment, I consider that the following contextual factors should be taken into account when considering the privacy issues and the application of the CDR to the telecommunications sector:

- the inherent sensitivity of information handled by telecommunications providers
- the potential for cross-sector combination of data which will increase the sensitivity of all CDR data (including telecommunications data), and
- evidence that the levels of community trust in relation to telecommunications providers' handling of personal information are lower than some other sectors such as banking, as indicated by the OAIC's 2020 *Australian Community Attitudes to Privacy Survey*.

Telecommunications data is sensitive and paints a rich portrait of a consumer's life

Telecommunications providers handle a wide range and large volume of personal information in the course of providing services to their customers. This includes customer contact information, usage information, information about the contents and substance of communications (pursuant to a warrant for law enforcement purposes),[2] as well as what is commonly referred to as 'metadata' (such as the time, location and recipient of a customer's communications).

All these types of information can reveal rich insights about a consumer, with metadata in particular having the potential to create a detailed picture of a consumer's personal life. Metadata can provide information about individuals' relationships and networks and frequently visited locations. This can map out an individuals' intentions through pattern recognition of their daily habits and movements. [3] The conclusions that may be inferred from metadata may reveal

[2] See generally Chapter 2 of the *Telecommunications (Interception and Access) Act 1979*.

[3] The OAIC has outlined these privacy impacts in several public submissions. See, eg, the OAIC's Review of the mandatory data retention regime — submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) (July 2019); Submission on the Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (January 2015), in particular Appendix A, which summarises studies into the privacy impacts of collecting metadata.

sensitive information about the individual, including information about an individual's health, political opinions, sexual orientation and circumstances of vulnerability.[4] The potential for harmful impacts can also be amplified for vulnerable consumers. The risks that the collection and retention of such data pose to an individual's right to privacy has been well-known for some time, and was specifically identified by the Joint Parliamentary Committee on Human Rights in 2014.[5]

Data sensitivity will be increased as CDR data from multiple sectors is combined

The sensitivity of, and privacy risks posed by metadata and other customer information handled by telecommunications providers should be considered in the context of the future potential cross-sector combination of CDR data.

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. More generally, the privacy risks associated with the use of telecommunications data need to be considered with reference to the broader context of increasing data use and amalgamation, in which data analytics and other data aggregation activities may be used to generate sophisticated insights in relation to and between data sets.

In light of this, I agree with the considerations relevant to vulnerable consumers as outlined on page 29 of the paper, but note these risks exist for all consumers (but are exacerbated for vulnerable consumers).

Community trust should inform the design of any instrument and privacy settings for the telecommunications sector

Regard should also be had to the community's attitudes to handling of personal information by the telecommunications sector to inform the privacy settings and design of any instrument. The community's attitudes to privacy are influenced by the trust afforded to the entity handling personal information, as well as the context and reason for the information handling. I note that there is evidence that a lower level of trust in the community exists regarding the handling of personal information by telecommunications providers. In OAIC's 2020 *Australian Community Attitudes to*

[4] Certain telephone numbers are used for a single purpose, such that any contact reveals basic and often sensitive information about the caller. Examples include support hotlines for victims of domestic violence and rape, or people considering suicide. There are specific services for first responders, veterans, and LGBTQI teenagers. Hotlines exist for sufferers of various forms of addiction, such as alcohol, drugs, and gambling. Regular calls to healthcare service providers may reveal underlying health concerns or personal issues that an individual is experiencing.

[5] See Parliamentary Joint Committee on Human Rights, Fifteenth Report: Examination of legislation in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011, at paragraph [1.34].

Privacy Survey, only 35% of respondents said that telecommunications providers were either very or somewhat trustworthy in relation to their handling of consumers' personal information, and 38% found the industry somewhat or very untrustworthy. This is lower than the trust level reported in other organisations, such as financial institutions (banks) and health service providers.[6]

Security risks in the telecommunications sector (re: Consultation Question 11)

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. This could increase the risk of unauthorised access to or disclosure of telecommunications data, for example due to hacking, identity theft and other fraud incidents, absent strong safeguards. The Office of the Australian Information Commissioner (OAIC) is also aware of existing security issues in the telecommunications sector, such as 'mobile porting fraud',[7] which may be impacted by the application of the CDR.

While the paper notes the existence of the sector-specific security obligations in the *Telecommunications Act 1997* (Telecommunications Act), I note the paper does not explore any sector-specific security risks. I therefore recommend that the privacy impact assessment for the proposed implementation of the CDR in the telecommunications sector explore sector-specific security risks, including by considering any feedback received from industry in response to this consultation, and whether those risks are able to be appropriately mitigated.

Recommendation 1 – That the privacy impact assessment explore sector-specific security risks, including by considering any feedback received from industry.

[6] In relation to financial institutions: 50% of respondents said that financial institutions were either very or somewhat trustworthy in relation to their handling of consumers' personal information, and 28% found the industry somewhat or very untrustworthy. In relation to health service providers: 70% of respondents said that health service providers were either very or somewhat trustworthy in relation to their handling of consumers' personal information, and 11% found the industry somewhat or very untrustworthy. See Figure 33 at B.8 of the OAIC's 2020 *Australian Community Attitudes to Privacy Survey* for further information.

[7] 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.

Classes of data for the telecommunications sector (re: Consultation Questions 4 and 11)

The paper sets out two categories of possible telecommunications datasets that may be designated to be available under the CDR on page 16: consumer data and product data. On page 27, the paper further explores potential classes of consumer data that could be designated, namely usage information, location data and information protected under Part 13 of the Telecommunications Act and the mandatory data retention scheme in the *Telecommunications (Interception and Access) Act 1979* (Interception Act).

For the purposes of this consultation, I have considered the potential consumer datasets only. I have not considered product data, because I understand this to be data for which there are no CDR consumers,[8] which would not raise issues relating to privacy or confidentiality of consumers' information.

In terms of the consumer datasets outlined on page 16, I am unable at this stage to provide a view on whether I generally support the designation of these datasets. This is because it is unclear from the paper as to whether the 'descriptions' of each class are exhaustive. For example, while I understand that the 'usage information' class would not include '…information related to whom communications were made to, or details of the messages',[9] it is unclear whether other information, such as the time and duration of communications, might be captured.[10] (As outlined below, my preliminary view is that these details, commonly referred to as 'metadata', should be not be designated as CDR data.)

I consider further detail and clarity on the proposed datasets needs to be given as part of the formal sector assessment report required to be published under section 56AE – this will assist me in considering the privacy impacts more fulsomely as part of my analysis and reporting obligations in section 56AF. I have however provided some comments in relation to the 'fees and charges' dataset which is proposed to be designated (see below under 'Information about financial hardship and other concessional arrangements').

---

[8] See, eg, note 4 to s 56AI(1) of the Competition and Consumer Act, which provides that CDR data for which there are no CDR consumers is also known as 'product data'. See s 56AI(3) for when a person will be a CDR consumer for CDR data.

[9] See page 27 of the paper.

[10] Such information is required to be retained under the Interception Act, and the paper notes Treasury is considering such data as a potential class of data to be designated for the telecommunications sector: page 28.

In terms of the classes of data dealt with on page 27 (i.e. those that Treasury considers may give rise to particular privacy impacts), I set out my views in the following sections. In formulating these preliminary positions, I have considered whether it would be reasonable, necessary and proportionate to designate a class of data as CDR data to achieve the policy objectives of the CDR,[11] including whether there are particular classes of data that, based on the information available at this stage, present privacy or confidentiality risks that may not be able to be mitigated to the appropriate extent, such that they should not be designated as CDR data.

Location data

It appears from the paper that Treasury considers location data to be '[m]obile location data [which] comes from a variety of sources including GPS signals, Bluetooth beacons and carrier mobile towers'.[12]

Location data is currently regulated by the Interception Act and Telecommunications Act. The Interception Act describes location data as including the location of equipment, or a line, used in connection with a communication, at the start and end of the communication (e.g. cell towers, Wi-Fi hotspots).[13] The Telecommunications Act defines 'location information' as being information or a document about the location of a mobile telephone handset or any other mobile communications device.[14]

It is unclear from the paper whether Treasury intends to align with these existing interpretations. For the purposes of this consultation and these comments, I understand 'location data' to be as per the description in the Interception Act (which appears broader than 'location information' as defined in the Telecommunications Act).[15] I consider that for the purposes of potential designation, the definition of 'location data' should be clarified as part of the formal sector assessment report

---

[11] See the Attorney-General's Department's template for a Statement of Compatibility for a Bill or Legislative Instrument that raises human rights issues. Page 2 of this template suggests that, when assessing the likely impact on the rights engaged, it should be explained why the limitation on the right is 'reasonable, necessary and sufficiently precise to ensure that it addresses only those matters that it is intended to capture as well as any relevant safeguards'. Relevant considerations include 'whether there are less restrictive alternatives for achieving the objective and whether they have been tried and whether sufficient regard been paid to the rights and interests of those affected'.

[12] Page 28.

[13] See Item 6 of s 187AA of the Interception Act.

[14] Section 275A of the Telecommunications Act

[15] For example, item 6 of s 187AA in the Interception Act ('location data') would include a range of communications (i.e. as it refers to the location of equipment or a line used in connection with 'a communication') whereas 'location information' in s 275A of the Telecommunications Act is explicitly limited to 'mobile telephone handsets' and 'mobile communications devices'.

required to be published under section 56AE. I note any such clarifications may influence the comments I make as part of my analysis and reporting obligations in section 56AF.

Information about the availability of a network in different locations and which technology is available at a particular location is proposed to be designated as 'product data'.[16] For completeness, given my understanding that such data, being product data, would not be data for which there are any CDR consumers, [17] I do not include such data in my interpretation of 'location data' for the purposes of these comments.

As outlined in the paper, location data is often regarded as inherently sensitive, due to the potential for this data to be used to identify an individual telecommunications user by drawing insights from the individual's location, or to track an individual.[18] I agree with this, and note that location data has a particularly high privacy impact as beyond showing where an individual has been, it can also reveal sensitive information about them such as information about their health and political or religious beliefs. It is also difficult to make such data anonymous.[19] There is a high level of regulation of telecommunications data in recognition of these impacts, and access can only be provided to law enforcement in strictly controlled circumstances.

There is significant community concern about the collection, use and disclosure of location data – for example, the OAIC's 2020 *Australian Community Attitudes to Privacy Survey* showed that 62% of Australians are uncomfortable with digital platforms and other online businesses tracking their location through their mobile or web browser, with 37% being 'very uncomfortable'.[20] The privacy risks and concerns would likely be increased in this context, where location data could be combined and analysed with other CDR data (e.g. banking data).

Given the sensitivity of location data (both perceived and actual), the OAIC has recently recommended that in certain contexts a full or partial prohibition on the

[16] See page 18 of the paper.

[17] See, eg, note 4 to s 56AI(1) of the Competition and Consumer Act, which provides that CDR data for which there are no CDR consumers is also known as 'product data'. See s 56AI(3) for when a person will be a CDR consumer for CDR data.

[18] Page 28.

[19] Anna Johnston (12 November 2020) 'Location, location, location: online or offline, privacy matters', *Salinger Privacy blog*

[20] See the OAIC's 2020 *Australian Community Attitudes to Privacy Survey* for further information.

handling of location data about individuals be introduced into the *Privacy Act 1988* (Privacy Act).[21]

The paper notes that the requirement for express consent to the sharing of location data recognises the importance of these privacy issues in the CDR context.[22] While I support the existing consent framework in the CDR system as an important privacy protection, I note that consent has limitations, particularly in light of the various challenges and complexities created by digital technologies.[23] Consent should be complemented by data handling restrictions and safeguards where the data is inherently sensitive.

As such, express consent may not in and of itself be able to mitigate against the privacy risks of sharing location data. Depending on the circumstances, issues may arise about a consumer's ability to provide fully informed and voluntary consent, for example where location data is reasonably needed to provide a CDR good or service (and a consumer's only option if they do not wish to provide this data, is not to engage with the product or service).[24] These challenges and the potential for harmful impacts can be amplified for vulnerable consumers.

The paper notes that there may be use cases for location data that could generate significant benefits for business and individual consumers and society more generally (e.g. transport planning).[25] While I acknowledge this, on the basis of the information available at this point I consider an individual's location data presents privacy or confidentiality risks that may not be able to be mitigated to the appropriate extent. I am particularly aware of the strict legislative controls currently in place for the retention of and access to telecommunications data for law enforcement purposes, and the need to ensure the integrity of those safeguards.

If Treasury is minded to consider the inclusion of location data further, the PIA should closely consider those regulatory safeguards and their implications.

---

[21] See Recommendation 40 on page 16 and commentary on page 42 of the OAIC's Submission to the Privacy Act Review – Issues Paper (December 2020).

[22] Page 28.

[23] For an overview of these limitations and how they constrain the usefulness of consent as a privacy protection, see paragraph 5.18 of the OAIC's Submission to the Privacy Act Review – Issues Paper (December 2020).

[24] In such a situation, although a consumer must be enabled by the accredited person to actively select each type of data they wish to share, a consumer may in practice be presented with a 'take it or leave it' proposition.

[25] Page 19.

Based on the information available at this time, my preliminary recommendation is that location data be expressly excluded from the definition of CDR data in the designation instrument.

Information required to be retained under the Interception Act ('metadata')

Telecommunications service providers are required to retain data as set out in section 187AA of the Interception Act, under Part 5-1A of that Act.[26] This includes information such as the source, destination, date, time, duration, type and location of a communication.[27] For the purposes of these comments, I refer to this data as 'metadata'.

As outlined earlier, there are significant privacy risks associated with the handling of metadata. As with location data, I do not consider express consent would in and of itself mitigate the privacy risks of sharing metadata.

The inherent sensitivity of and privacy risks associated with this data have been recognised by the Interception Act, which tightly regulates access to metadata: while certain authorised officers in agencies may request that telecommunications service providers provide this data as part of investigations into crime, revenue and national security matters, access to metadata may only be requested once specific legal requirements have been met.[28] Further, requests for access to data are subject to independent oversight by the Commonwealth Ombudsman.[29] The OAIC also conducts assessments of the handling of this data and record keeping requirements of Telecommunications providers.[30]

There are stringent security obligations imposed on providers regarding metadata under the Interception Act (which, amongst other things, require entities to encrypt

---

[26] See in particular s 187A of the Interception Act.

[27] See s 187AA of the Interception Act. Service providers were given 18 months to upgrade their systems to meet the retention and encryption requirements under the Interception Act (see Division 2 of Part 5-1A, which outlines the process for approval of 'data retention implementation plans', being the plans in which providers outlined the interim arrangements to be implemented (to the extent that the information and documents would not be kept in compliance with the data retention regime, including the security requirements), and specified the day by which they would comply with the data retention requirements).

[28] See generally Chapter 4 of the Interception Act, in particular s 180F which requires an authorised officer to be 'satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use [of metadata] is justifiable and proportionate', having regard to several matters including the gravity of any conduct in relation to which the authorisation is sought.

[29] See generally Chapter 4A of the Interception Act.

[30] See information on the OAIC's website relating to the Australian Information Commissioner's role in the regulation of the Telecommunications industry.

metadata).[31] In addition to technical complexities,[32] there are likely to be regulatory complexities in designating metadata as CDR data, for example, because of the numerous legislative requirements that would apply to this data (across the CDR framework, Interception Act and Privacy Act at a minimum).[33]

More generally, and particularly in the absence of compelling policy arguments for designating such data or use-cases which suggest significant consumer benefit,[34] I consider that it may not be reasonable, necessary and proportionate to designate all metadata as CDR data to achieve the policy objectives of the CDR.

My preliminary recommendation is that metadata be expressly excluded from the definition of CDR data in the designation instrument.[35]

If Treasury is minded to consider the inclusion of meta data further, the PIA should closely consider each kind of data, the use case, and whether current regulatory safeguards over the data can be maintained.

Information protected under Part 13 of the Telecommunications Act

Part 13 of the Telecommunications Act regulates the use and disclosure of certain information by eligible persons (such as carriage service providers and telecommunications contractors),[36] including any information or document that relates to the contents or substance of a communication[37] (often referred to as 'content' data) as well as location data.[38] As I have dealt with location data in the above section, my comments here are in relation to other, non-location information regulated under Part 13 of the Telecommunications Act.

---

[31] See s 187BA(a) of the Interception Act.

[32] Service providers were given 18 months to upgrade their systems to meet the retention and encryption requirements under the Interception Act (see Division 2 of Part 5-1A, which outlines the process for approval of 'data retention implementation plans', being the plans in which providers outlined the interim arrangements to be implemented (to the extent that the information and documents would not be kept in compliance with the data retention regime, including the security requirements), and specified the day by which they would comply with the data retention requirements).

[33] Telecommunications data collected under the data retention scheme in the Interception Act is deemed to be personal information within the meaning of the Privacy Act: see s 187LA of the Interception Act.

[34] The paper notes on page 19 that there may be use cases for location data that could generate significant benefits for business and individual consumers and society more generally (e.g. transport planning). However the paper does not explore use cases for other types of metadata.

[35] For clarity, I note that there may be some 'general' types of data required to be kept under the Interception Act, which I am not referring to here, for example, name and address.

[36] See s 271 of the Telecommunications Act.

[37] See, eg, s 276 of the Telecommunications Act.

[38] See s 275A of the Telecommunications Act.

Stored communications which reveal the content and substance of an individual's communications with others have traditionally been viewed to entail even greater privacy sensitivity than metadata,[39] sometimes referred to as 'non-content' data. However, rapid technological developments have increasingly blurred the distinction between 'content' data and 'non-content' data, as well as the distinction between what is and is not identifiable of an individual.[40] In addition, it would appear that there is a clear legislative intent for use and disclosure of content data to be tightly proscribed.[41]

In light of this, I recommend that information protected under Part 13 of the Telecommunications Act be expressly excluded from the definition of CDR data in the designation instrument.

Information about financial hardship and other concessional arrangements

A 'fees and charges' class of consumer data is proposed to be designated, which would include 'discounts or other variations to fees and charges tailored to individual consumers'.[42] I understand this could include financial hardship information and other concessional arrangements and may be highly sensitive to consumers in that it could reveal insights about their financial capacity which could, for example, influence the goods or services that are subsequently offered to a consumer.

Unless evidence is received during consultation that this is required for potential use-cases with strong consumer benefit, our preference would be for financial hardship information and information about other concessional arrangements to be excluded from 'fees and charges', such that it cannot be CDR data.

If evidence is received that supports the case for inclusion of this data, it will be important to ensure that appropriate mitigation strategies are in place, for example to ensure the consumer data standards present financial hardship/concessional information as a standalone data cluster (instead of being bundled with other 'fees

---

[39] See, eg, the Explanatory Memorandum to the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, at page 66.

[40] See, eg, David Vaile, Shavin Wijeyaratne, Genna Churches, Monika Zalnieriute, Allens Hub for Technology, Law and Innovation, Submission to the Parliamentary Joint Committee on Intelligence and Security inquiry into the mandatory data retention regime, UNSW Law Research Series (July 2019) at page 5.

[41] See, eg, s 280 of the Telecommunications Act. Although the use or disclosure of regulated information would be permitted where required or authorised by or under law (such as in response to a consumer data request under the CDR regulatory framework), such a use or disclosure would still not be permitted if any of the many situations in s 280(1B) apply.

[42] See page 17 of the paper.

and charges' data), so that consumers have sufficient control over whether or not to share this particular data.[43]

I would also recommend that the privacy impact assessment explore this issue further, including any particular impacts on vulnerable consumers.

Recommendation 2 – That location data, 'metadata' and information protected by Part 13 of the Telecommunications Act be explicitly excluded from the definition of CDR data in the designation instrument.

Recommendation 3 – That a cautious approach be adopted when considering whether to designate information about financial hardship and other concessional arrangements. Our preference at this stage would be for such information to not be designated as CDR data.

Recommendation 4 – That the privacy impact assessment explore the privacy issues associated with designating financial hardship/concessional information, including any impacts on vulnerable consumers.

Ways in which the extension of CDR should take into account existing regulation in the telecommunications sector (re: Consultation Questions 15 and 11)

I strongly support the suggestion in the paper that information regulated under Part 13 of the Telecommunications Act and the mandatory data retention scheme in the Interception Act should only be used and disclosed in accordance with those laws.[44]

As outlined earlier, my preliminary recommendation is that data required to be retained under the Interception Act, and data regulated under Part 13 of the Telecommunications Act, should not be designated as CDR data (leaving this data to be used and disclosed only in accordance with existing laws).

The boundaries of 'telecommunications data' and the 'telecommunications sector' (re: Consultation Questions 1 and 6)

The paper queries the extent to which the telecommunications sector should be defined to cover both the traditional telecommunication services and the complementary and related services that these services facilitate, such as entertainment, shopping, social interaction and medical services. This would mean

[43] I note this is the approach that is proposed to be adopted in relation to hardship information for the energy sector: see the 'Get concessions' heading in the CDR Energy Standards – DRAFT (0.2.0).

[44] Page 28.

other datasets, not traditionally viewed as 'telecommunications data' could be designated as CDR data for the telecommunications process, to provide a 'wrap-around' value proposition for consumers.[45]

I do not consider that datasets from other sectors (such as entertainment, shopping, social networks and health) should be part of designating the telecommunications sector as one to which CDR applies, due to the privacy and confidentiality implications that are specific to those sectors. I consider it would be more appropriate to consider datasets from these other sectors as part of separate sectoral assessments for the relevant sector, at the appropriate point in time. This would also allow the privacy and confidentiality issues for those datasets to be considered in full, and with regard to the broader context of what other datasets are proposed to be designated for those particular sectors.

I note that the Treasury's strategic assessment is seeking views on including a wide array of sectors and datasets such as the digital platforms and health sectors as part of the future rollout of the CDR, which would encompass some of these complementary and related services. I generally support this approach of considering these sectors and datasets individually so that their specific privacy and confidentiality implications may be appropriately considered.

In addition, any expansion of the 'telecommunications sector' and 'telecommunications data' in the manner outlined in the paper would likely lead to an increasingly complex data sharing model with associated risks, as more data holders would be required to share data to fulfil a single consumer data request. (The proposed data sharing model already requires coordination between multiple data holders from the 'traditional' telecommunications sector.[46])

Finally, while the Competition and Consumer Act would not preclude such an approach,[47] I consider that Treasury should adopt an interpretation that is consistent with general and broadly accepted understandings of what constitutes the telecommunications sector and/or industry.[48] This would assist regulated entities to

[45] See pages 8 and 20.

[46] See pages 31 to 34 of the paper.

[47] The Competition and Consumer Act does not define 'sector', and only broadly defines a 'designated sector' as 'a sector of the Australian economy designated under subsection [56AC](2)': ss 4 and 56AC(1) of the Competition and Consumer Act.

[48] See, eg, the membership of the Telecommunications Industry Ombudsman, which includes telecommunications service providers (including carriers and eligible carriage services providers) (https://www.tio.com.au/about-tio) and the persons regulated by key legislation in this sector including the Telecommunications Act and Interception Act.

more easily comply with their obligations under the CDR system, as it would build on pre-existing understandings.

Recommendation 5 – That for the purposes of sectoral designation, the telecommunications sector be understood to encompass traditional telecommunication services only, and not complementary and related services.

Proposed 'peer-to-peer' model for data sharing (re: Consultation Question 13)

The paper notes that a peer-to-peer model, similar to the model being implemented for the energy sector, is potentially appropriate for the telecommunications sector, as this would ensure interoperability and consistency between sectors and provide a solution where relevant datasets for a consumer are held by more than one potential data holder (as would appear to be the case in the telecommunications sector).[49]

The key objective for the OAIC regarding any data sharing model in the telecommunications sector is to ensure that the model is implemented in a way that ensures the privacy and security risks are minimised and managed across the scheme, such that a consistent and appropriate level of protection exists for consumers' CDR data (regardless of which sector the participants belong to), and the overall integrity of the privacy protections in the CDR system is maintained. I would also like to ensure the consumer experience of using the data sharing model is as consistent as possible across sectors (as a consistently better experience for consumers supports informed consent, which leads to better privacy outcomes overall).

On this basis, I support the focus on ensuring consistency between sectors. OAIC staff would be happy to work with Treasury staff to help identify and address any relevant privacy impacts of proposed data sharing models at the appropriate point in time, when further detail is available.

In addition, I generally agree that a centralised data sharing model, in which one data holder would collect and disclose data to accredited data recipients, is unlikely to be appropriate for the telecommunications sector. Further, I understand that a centralised model would likely require the creation of a new entity, or expansion of an existing entity's functions, to fulfil this role.[50] The creation of a new entity in

[49] Page 32.

[50] This is because it would be 'difficult to identity a suitable sole data holder' for the telecommunications sector given the particularities of how datasets are held by multiple entities and the lack of a centralised identity provider: see page 32 of the paper.

particular could raise new privacy and security risks, by increasing and changing data flows between relevant entities.

Were an existing entity's functions to be expanded, privacy risks may arise from that entity needing to broaden their personal information holdings or the purposes for which they handle consumer data. Any such risks would need to be mitigated through appropriate data handling restrictions, and should be considered in detail as part of further privacy impact assessments at the appropriate point in time.