September 2018

CDR exposure draft legislation – OAIC submission to The Treasury

*Treasury Laws Amendment (Consumer Data Right) Bill 2018*

Contents

[Introduction 3](#_Toc524943850)

[About the Office of the Australian Information Commissioner 4](#_Toc524943851)

[CDR and the interaction with the credit reporting provisions in Pt IIIA of the Privacy Act 4](#_Toc524943852)

[Providing further clarity around the key principles for the framework 5](#_Toc524943853)

[The boundaries of the CDR regulatory scheme 5](#_Toc524943854)

[Balance between legislation and rules 6](#_Toc524943855)

[Non-accredited recipients 8](#_Toc524943856)

[Regulation of de-identified information 8](#_Toc524943857)

[Scope of the OAIC’s regulatory role 9](#_Toc524943858)

[Complaint handling for different types of consumers 9](#_Toc524943859)

[OAIC’s regulatory powers should extend to certain Rules 9](#_Toc524943860)

[OAIC’s ability to investigate privacy safeguard 1 breaches 10](#_Toc524943861)

[Other comments 10](#_Toc524943862)

## Introduction

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the exposure draft of the *Treasury Laws Amendment (Consumer Data Right) Bill 2018* (the Bill) and the exposure draft of the Explanatory Memorandum to the Bill (EM).[[1]](#footnote-1)

By way of an overall comment, the OAIC welcomes the introduction of the Consumer Data Right (CDR) and is strongly supportive of initiatives which seek to give individuals greater choice and control over how their data is used. The OAIC also acknowledges the other important policy objectives behind the introduction of CDR, which include ensuring that individuals can use their data to enable the provision of new or improved services, to increase competition, and to drive innovation.

The intention as reflected in the exposure draft is for both the Australian Competition & Consumer Commission (ACCC) and the OAIC to have roles in regulating the CDR scheme. The OAIC and the ACCC have already begun working together on preliminary implementation matters, and the OAIC looks forward to continuing to work with the ACCC to deliver a scheme that achieves its broader competition objectives, while ensuring strong privacy and information security protections.

As the scheme is intended to facilitate individuals sharing their data with third parties, it will inevitably lead to increased information flows between participating entities (such as banks and financial institutions in the case of open banking), meaning the CDR scheme will therefore have significant implications for the handling of individuals’ personal information. It is important that a strong framework for privacy protection is in place, in addition to strong security and identity verification measures, to ensure that the risk of misuse and improper disclosure, particularly fraud, is minimised.[[2]](#footnote-2) A strong privacy and security framework is necessary not only for protecting consumers’ information, but also for maintaining public confidence in, and the integrity of, the CDR scheme. The OAIC therefore welcomes the Bill and EM’s clear focus on incorporating privacy protections, and ensuring data protection considerations are a central part of the legislative framework.

The comments in this submission identify a number of areas in the Bill and EM where the OAIC considers that further clarification or consideration of privacy issues is required. Broadly, these areas relate to:

* the CDR scheme’s interaction with Part IIIA (the credit reporting provisions) in the *Privacy Act 1988* (Cth) (Privacy Act)
* clarifying certain basic principles and aspects of the regulatory framework
* the regulation of de-identified information
* the role of non-accredited data recipients, and
* the OAIC’s regulatory role.

### About the Office of the Australian Information Commissioner

The OAIC is an independent statutory agency within the Commonwealth Attorney-General’s portfolio. The Australian Parliament established the OAIC in 2010 to bring together three functions:

* privacy functions (regulating the handling of personal information under the Privacy Act(and other Acts))
* freedom of information functions, including access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982* (Cth)
* information management functions.

The integration of these three interrelated functions into one agency provides the OAIC with a unique perspective, as it seeks to balance the right to privacy with broader information policy goals.

The Privacy Act confers a range of regulatory powers on the Commissioner, including powers that allow the OAIC to work with entities to facilitate legal compliance and best privacy practice, as well as investigative and enforcement powers. The regulatory powers are based on an escalation model.[[3]](#footnote-3)

As part of its privacy functions, the OAIC regulates the handling of personal information under the Privacy Act, which includes the thirteen Australian Privacy Principles (APPs). This includes regulating APP 12, which currently gives individuals the ability to access and receive a copy of the personal information held about them by agencies and organisations, subject to some exceptions. As set out in the EM, the CDR builds on APP 12 by providing consumers with the ability to direct data transfers to third parties, to access information about the transactions they enter into, to access information relating to products, and by applying to business consumers as well as individuals.[[4]](#footnote-4)

## CDR and the interaction with the credit reporting provisions in Pt IIIA of the Privacy Act

The initial rollout of the CDR scheme will be in the banking sector, and will therefore facilitate the transfer of individuals’ banking data directly from their current providers to third parties. Under the existing arrangements in Part IIIA of the Privacy Act, the situations in which some of the same types of information may be shared are specifically prescribed and limited.[[5]](#footnote-5) However, the CDR scheme will significantly expand the situations in which this information may be shared outside of the Part IIIA framework.

The expected interaction between the CDR scheme and the credit reporting provisions under Part IIIA is briefly addressed in s 56EC(3) of the Bill, which states that *‘[s]ubject to the regulations, this Division does not limit Part IIIA (about credit reporting) of the Privacy Act 1988’*. While the CDR scheme may not limit Part IIIA, in our view the implications of the CDR scheme on the underlying policy objectives of Part IIIA should be considered more fully.

For example, Part IIIA seeks to achieve a balance and ensure that appropriate consumer protections are in place in relation to the handling of credit information, recognising the significant impact that decisions about creditworthiness can have on individuals. It does this by prescribing the types of information that can flow between credit providers and credit reporting bodies for use in assessing an individual’s creditworthiness, by limiting the types of bodies which can access this information, and by limiting which types of credit information certain credit providers can access.[[6]](#footnote-6)

By contrast, the current Bill provides that the rules will determine which entities can be CDR data recipients, and what CDR data they can access, without providing further guidance on what limits may be necessary or appropriate. While the CDR reforms are intended to be consumer driven and to enhance competition, it is important to be aware that, in the absence of appropriate limitations, there is a risk that the consent element of CDR may be undermined, and may lead to unfair or unintended consequences for individual consumers, particularly those who are vulnerable. For example, while CDR data can only be transferred to a third party with the affected individual’s consent, in the absence of more specific limitations, data recipients may begin requiring individuals to provide their CDR data as a pre-condition for having their application for a particular product or service considered.

Accordingly, we recommend that consideration be given to whether any additional consumer safeguards need to be included in the Bill as a result of the changes to be brought about by the CDR scheme,[[7]](#footnote-7) in particular in relation to the potential disclosure of banking data to non-accredited recipients.[[8]](#footnote-8) For example, consistent with the approach in Part IIIA, there may be specific types of entities that should be explicitly prohibited from collecting CDR (and in particular, banking) data.

On a related note, the introduction of CDR may also present an opportunity to consider whether other methods of providing access to sensitive financial data, particularly screen scraping, should be restricted in light of the availability of the more secure and protective CDR method. While the OAIC acknowledges that the Review into Open Banking (OB report) viewed screen scraping as ‘an important market-based check on the design of Open Banking’,[[9]](#footnote-9) the OAIC also considers that there may be cases where vulnerable individuals may be in need of extra protection.

## Providing further clarity around the key principles for the framework

### The boundaries of the CDR regulatory scheme

To ensure there is certainty around the regulatory requirements for all CDR participants, it is important that there is clarity around when the APPs apply to each type of CDR participant, and when the privacy safeguards apply. In our view, the current Bill is in need of further refinement to ensure sufficient clarity is provided on these issues.

In particular, the OAIC notes that the boundaries of the CDR scheme, and when it will apply to the handling of CDR data, do not appear to be clear on the face of the Bill.[[10]](#footnote-10) From a regulatory perspective, it is critical to clearly identify the boundaries of the CDR scheme, to ensure that regulated entities are clear about when the privacy safeguards will apply, and when APP coverage resumes. The intended position appears to be reflected in Example 1.14 in [1.177] of the EM. This states that if a consumer decides to become a customer of an entity that received their data as an accredited data recipient, ‘*all new transaction data created by [the entity] in relation to [the customer’s] transaction account is subject to the Privacy Act and the APPs’*.[[11]](#footnote-11)

In order to provide regulatory certainty for CDR participants, the OAIC recommends that the legislation itself expressly defines the boundaries of the CDR regulatory scheme. Alternatively, the EM should explain how the provisions of the Bill operate to define this boundary, rather than explaining the policy position through an example. Without providing greater certainty around when the CDR framework stops applying, there is a risk that industry may have difficulty applying the scheme in practice. In particular, as CDR is necessarily more prescriptive than the APP framework, its scope needs to be clearly defined to ensure that ongoing customer or business relationships are able to be governed with sufficient flexibility (i.e. under the less prescriptive APP regime).

In addition, the OAIC recommends that the Bill itself sets out how the APPs and privacy safeguards interact for both data holders and accredited data recipients (or alternatively, that the EM explain how the provisions of the Bill currently operate to achieve the regulatory outcome).[[12]](#footnote-12) Based on statements in the EM, the OAIC understand that data holders will continue to have obligations under the APPs, with certain privacy safeguards imposing *additional* requirements once a data holder receives a transfer request. In contrast, the privacy safeguards apply *instead of* the APPs for accredited data recipients while the information is being handled within the CDR scheme.[[13]](#footnote-13) This outcome is not apparent on the face of the Bill, nor does the EM appear to explain how the Bill operates to achieve this outcome.

### Balance between legislation and rules

Much of the detail of the CDR scheme requirements is being left to the discretion of the rule-maker, as acknowledged in the EM (for example, see [1.27] and [1.111]). The explanation for this approach is that, given the CDR will be applied across very different sectors of the economy, flexibility is needed to make rules that are appropriate and adapted to any industry that might become designated in the future.

The OAIC acknowledges the need to tailor the regulatory framework for different sectors as the CDR is rolled out across the economy. However, the OAIC recommends that further consideration be given to the balance between the legislation and rules in some instances. For example, we note that the EM states that *‘…the consumer data rules will be the primary mechanism through which consumers and their data are protected’* [1.163]. Given that consumers’ privacy and data protection are fundamental to the success of the CDR scheme, in our view, to provide certainty and clarity, the primary legislation should set out in greater detail what the Rules should cover rather than leaving these matters to the discretion of the rule-maker.

#### Discretionary rule-making

The rule-making powers in the Bill are expressed as *‘The Commission* ***may****…’* make certain rules.[[14]](#footnote-14) Given the level of detail being left to the rules, in our view it would be more appropriate for the rule-making power to be mandatory.

#### Key principles being left to the rules

While the OAIC acknowledges the need for the Bill to be flexible enough to accommodate sectoral differences, there appear to be elements of the regulatory framework that the Bill proposes leaving to the rules, which may in fact not need to differ between sectors. For example, some of the intended features for safeguards of the scheme could be included in the primary legislation, at least at a high level, to guide the making of the Rules. For example:

* The legislation contains no requirements about what constitutes consent, notwithstanding that the OB Report recommended consent must be express, and the Treasury material[[15]](#footnote-15) about the CDR scheme more generally also noted that consent must be clear and unambiguous (rather than implied). As the policy decision is that express consent is needed across all CDR sectors, we recommend this is reflected in the legislation.
* The Bill does not expressly provide a ‘right’ to request the transfer of data. Rather, the Bill provides a broad discretion to the rule-maker to make Rules which may cover the transfer of data. As the right to request the transfer of data to trusted third parties is the fundamental concept underlying the CDR, we recommend including it in the legislation.
* While some privacy safeguards are more prescriptive than others, some leave all or significant detail to the rules. This particularly applies in relation to privacy safeguard 5 (notifying of the collection of CDR data). It is not clear on the face of the Bill or EM whether there is a need to allow for such a high degree of flexibility between sectors. By contrast, the APPs, which are principles-based and operate across all sectors, contain significantly more prescription than privacy safeguard 5. We therefore suggest that consideration be given to including a list of minimum notification requirements within privacy safeguard 5, with the rules then able to add additional notification requirements for particular sectors if required.

#### Relationship between legislation, rules and standards

By way of general comment, the relationship between the legislation, rules and standards is not sufficiently clear in all cases. For example, for privacy safeguard 11, it is not clear how breaches of the data standards will feed into breaches of the safeguards or rules. The OAIC recommends that further consideration be given to ensuring this relationship is made clear within the legislation.

## Non-accredited recipients

The privacy safeguards apply to a recipient only where they are an ‘accredited data recipient’.[[16]](#footnote-16) However, the possible role of non-accredited data recipients is not clear on the face of the Bill, even though the existence of non-accredited recipients is flagged in the EM.

For example, the EM states that the system is flexible and the rules can allow *‘for interactions between consumers and non-accredited entities’* (see [1.26]). It goes on to say *‘In certain circumstances, CDR consumers can direct that their CDR data be provided to a non-accredited entity. Data that has been derived from CDR data, such as financial reports compiled from transaction data, may also be transferred by a CDR consumer out of the CDR system. For example, to their accountant’* (see [1.47]).

As set out in the OB Report, the intention for the CDR scheme was to facilitate the transfer of information to trusted third parties. Given that disclosures to non-accredited recipients would be a departure from this general intention, we recommend that the EM more clearly explain the policy intention behind allowing such disclosures. Our earlier comments in relation to the CDR scheme’s interaction with the Part IIIA framework also apply here.

In addition, as the privacy framework that would apply to such disclosures would differ to the CDR framework applying to general CDR disclosures, it is important that disclosures to non-accredited recipients be allowed only in limited circumstances. Consumers should also be clearly notified that the disclosure is occurring, and that the CDR privacy protections will not apply.

## Regulation of de-identified information

Section 56AA(b) states that an object of Part IVD is *‘to enable any person to access any information in those sectors that does not relate to any identifiable, or reasonably identifiable, consumers’*. Further, section 56BD provides a very broad power to make rules, including in relation to data which has been subject to de-identification or aggregation processes, without providing any further guidance about what the limits of an ‘open data’ approach to the CDR scheme should be (that is, an approach which may involve the open sharing or publication of CDR data).[[17]](#footnote-17)

It may be appropriate to promote an open data approach in relation to data that was never about a consumer, such as information about product offerings. However, we would caution that undertaking de-identification or similar processes in relation to data about individual consumers (i.e. personal information) to a standard that would enable safe public release carries significant risks of re-identification and consequently, data breaches.

The OB Report emphasised that the intended core focus of the scheme is allowing consumers to share their data with trusted third parties only. As a move away from this more limited focus could potentially raise privacy and security concerns, in our view it would be appropriate for either the Bill or the EM to clarify that the CDR scheme is not aimed at enabling the open publication of data that is, or is derived from, personal information (i.e. individual consumers’ data).

## Scope of the OAIC’s regulatory role

### Complaint handling for different types of consumers

We understand that the OAIC will be responsible for handling privacy and confidentiality complaints made by individuals and small businesses (those with a turnover <$3 million), but not those made by larger businesses.[[18]](#footnote-18) However, this distinction in how complaints will be handled does not appear to be clear on the face of the Bill. In particular, Item 2 in the table to s 56ES(2) replaces references to ‘individual’ in Part V of the Privacy Act with ‘CDR consumer for the CDR data to which the privacy safeguard contravention relates’, but ‘CDR consumer’ includes large businesses. The OAIC therefore recommends that the Bill:

* make clear that the OAIC will only handle complaints made by individuals and small businesses, and
* outline the dispute resolution options for large businesses.

### OAIC’s regulatory powers should extend to certain Rules

The Bill provides that the OAIC’s current investigative and enforcement powers as set out in Part V of the Privacy Act are to be extended to breaches of the privacy safeguards (see s 56ES). Similarly, the OAIC will have a power to assess whether the handling of CDR data is in compliance with the privacy safeguards.

Under s 56BC(f), the rules to be made by the ACCC include rules relating to the privacy safeguards. Note 2 to that section states that *‘The rules may deal with similar or additional matters to those in the privacy safeguards’*.

As the primary privacy complaint handler, the OAIC will need to be able to enforce breaches of the CDR Rules in addition to breaches of the safeguards, where the Rules relate to the privacy safeguards. Where the rules are explicitly referenced within the privacy safeguards, a separate power to enforce the rules may not be necessary. However, our understanding of the Bill is that the rules may contain other provisions dealing with ‘similar or additional matters’. To ensure the OAIC is able to fulfil its role, and ensure all privacy breaches are handled by the same regulator, we recommend that the OAIC’s ability to regulate these breaches be clarified.

Along similar lines, we suggest that the OAIC’s assessment power in section 56EQ(1) should be extended so that it includes the power to assess whether CDR data is being maintained and handled in accordance with the privacy safeguards, and any rules relating to privacy. In order to be able to conduct a comprehensive assessment which provides useful education and recommendations to the CDR participant, it is important that the OAIC can also consider the rules which are relevant to the assessment scope.

By way of general comment on Note 2 to s 56BC(f), the phrase ‘similar or additional matters’ is ambiguous, and the note seems unnecessary in light of the breadth of the rule-making powers. We therefore recommend that this note be removed.

### OAIC’s ability to investigate privacy safeguard 1 breaches

Privacy safeguard 1 is a critical, foundational safeguard in that it ensures the open and transparent handling of CDR data. Importantly, it requires participants to implement practices, procedures and systems to ensure compliance with the privacy safeguards, and it requires the publication of a participant’s CDR policy to ensure its information handling practices are transparent. For this reason, it is important that the Information Commissioner can effectively investigate breaches of privacy safeguard 1.

Under the Privacy Act, breaches of APP 1 do not generally constitute an interference with the privacy of an individual, as APP 1 relates to an entity’s general policies and procedures relating to privacy. For example, an entity may breach the principle if it fails to have an up-to-date privacy policy (but this is unlikely to directly breach the privacy of a specific individual). However, the OAIC has the ability to initiate an investigation into any possible breaches of this APP, to ensure compliance (see s 40(2)(a)).

Section 56ES, which extends Part V of the Privacy Act to the CDR, would prevent the OAIC from investigating breaches of privacy safeguard 1 because s 56ES(3)(a) states that references in Part V to APP 1 should be disregarded.

To enable the OAIC to enforce breaches of privacy safeguard 1(consistent with its existing regulatory powers in relation to APP 1), we recommend that:

* the table in 56ES(2) be amended to add an additional reference to ‘a breach of APP 1’ being replaced with ‘a breach of privacy safeguard 1’, to allow the OAIC to investigate such breaches, and
* section 56ES(3)(a) should be deleted.

## Other comments

#### Technical matters - Section 56ES (Investigating breaches of the privacy safeguards)

Section 56ES(1)(a) refers to a CDR participant that ‘holds’ CDR data. However, we note that the definition of ‘interference with privacy’[[19]](#footnote-19) does not include a separate ‘holds’ requirement.[[20]](#footnote-20) The inclusion of this term therefore appears unnecessary, and could potentially lead to unintended consequences. The APPs and the privacy safeguards do not only apply where information is ‘held’, and the Commissioner needs to be able to investigate breaches that occur when data is not being ‘held’. For consistency with the Privacy Act, and to ensure that enforcing compliance with the privacy safeguards is not unnecessarily limited, we recommend that the term ‘holds’ be removed.

As an alternative to using the word ‘hold’, s 56ES(1) could be amended so that (a) reads ‘of a CDR participant’ and (b)(i) reads ‘the privacy safeguards in relation to a CDR consumer’s CDR data’.

In relation to s 56ES(1)(b)(ii), for consistency with the Privacy Act, we suggest the legislative references in this subparagraph include subsections as follows: s 26WH(2), s 26WK(2), s 26WL(3) or s 26WR(10).

The text at the end of s 56ES(1) states that Part V is intended to apply ‘in a corresponding way to the way that Part applies to an act or practice of an organisation, person or entity’. As Part V of the Privacy Act applies to acts or practices of ‘APP entities’, we recommend that the words ‘organisation, person or entity’ be replaced with ‘APP entity’.

#### Privacy Act definitions

The Bill uses some concepts which are defined in the Privacy Act such as ‘collects’ and ‘holds’. However, these definitions do not appear to be replicated in the *Competition and Consumer Act 2010* (Cth) (CCA). We recommend that the Bill either inserts these definitions into the CCA, or contains a section explaining that these (and any other relevant) terms are to be interpreted in accordance with the Privacy Act definition.

#### General approach – defining multiple data types

The Bill contains a number of definitions of data and related concepts. This includes the definition of CDR data and related definitions (s 56AF), data for which there are, and are no, CDR consumers (ss 56BC – BD), the data covered by the privacy safeguards (s 56EB), and ‘subject data’ (s 56EE and 56 EO (privacy safeguards 2 and 12)).

While we appreciate the need for specificity, this proliferation of definitions appears to result in a complex, and at times difficult to follow, framework. In our view, further consideration should be given to whether any of these definitions or concepts can be streamlined.

#### Australian Information Commissioner Act amendments

Items 3 and 4 of the Bill make amendments to the *Australian Information Commissioner Act 2010* (Cth) to include functions conferred on the Commissioner by Part IVD of the CCAwithin the definition of ‘privacy functions’.

In our view, the addition of the word ‘mainly’ into section 4 is ambiguous, and we would therefore recommend amending along the following lines:

‘the privacy functions, which are about protecting the privacy of individuals in accordance with the *Privacy Act 1988* (and other Acts), or the privacy of CDR consumers in relation to Part IVD of the *Competition and Consumer Act 2010’*.

#### Timeframes for correction

Privacy safeguard 12 (correction of CDR data) does not include any references to timeframes for responding to correction requests. To ensure that data holders and accredited data recipients respond promptly to correction requests, we suggest that the Bill reference timeframes. This could be achieved by stating that the entity must respond to the request within the timeframe specified in the consumer data rules or, if no timeframe is specified, within a reasonable period.

#### Foreign accredited data recipients

Following on from Recommendation 4.1 of the OB report, we understand there is a policy intention that all accredited data recipients be covered by the Privacy Act. Where this is the case, there will be no circumstances where the handling of personal information by an accredited data recipient is not protected by either the privacy safeguards, or the Privacy Act.

However, it is not clear whether the Bill would require all foreign entities who are able to obtain accreditation to be covered by the Privacy Act.[[21]](#footnote-21) The OAIC suggests that further consideration be given to this scenario.

#### EDR schemes and interaction with the OAIC’s role

The Bill empowers the ACCC to recognise EDR schemes to handle disputes about CDR. However, it does not specify how this will interact with the OAIC’s role as the complaint-handler (that is, that people can complain first to the relevant EDR scheme, and then to the OAIC). The OAIC suggests that this be clarified.

#### Fees

The Bill notes that the rules can enable fees to be charged for certain uses or disclosures (including transfers) of CDR data. The OAIC recommends that the Bill include a limitation that any fees which may be imposed are reasonable and not excessive.

#### Section 157AA(3) of the Competition and Consumer Act

Proposed section 157AA(3) of the CCA is a broad power for the Commission to disclose any information obtained under Part IVD or the consumer data rules to foreign agencies in similar roles. We note that this disclosure power appears to be very broad, and would recommend that this power to disclose be more limited. For example, the disclosures could be limited to situations where the individual consents, the information is relevant to an enforcement or similar function of that foreign agency, and where the Commission is satisfied the information will enable or assist that body to perform or exercise any of their functions or powers (as per the existing section 155AAA(12)(n) in the CCA).

1. Under the *Privacy Act 1988* (Cth) (Privacy Act), one function of the Privacy Commissioner is to examine proposed enactments that would require or authorise acts or practices of an entity that might otherwise be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals. The Commissioner also has the function of ensuring that any adverse effects of the proposed enactment on the privacy of individuals are minimised. See s 28A of the Act. [↑](#footnote-ref-1)
2. In relation to the banking sector, see the OAIC’s [*Notifiable Data Breaches Quarterly Statistics Report: 1 April - 30 June 2018*](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-quarterly-statistics-report-1-april-30-june-2018), which reveals that the finance sector was one of the top reporting sectors. [↑](#footnote-ref-2)
3. See the OAIC’s *Privacy regulatory action policy*: <https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/>. [↑](#footnote-ref-3)
4. See EM [1.11]. [↑](#footnote-ref-4)
5. See, for example, ss 20E-20F and 21G-21H of the Privacy Act. [↑](#footnote-ref-5)
6. For example, there are restrictions on landlords and real estate agencies accessing this information – see this OAIC fact sheet for further information: <https://www.oaic.gov.au/individuals/privacy-fact-sheets/credit-reporting/privacy-fact-sheet-29-who-can-access-your-credit-report>. In addition, telecommunication and utility providers are prohibited from accessing ‘repayment history information’ under Part IIIA arrangements (see s 21D(3)(c) of the Privacy Act). [↑](#footnote-ref-6)
7. For example, one consequence of the scheme could be that entities may require the provision of information available through the CDR, as a prerequisite for accessing certain products or services. While in some cases this may lead to consumers gaining a better deal, for others it may in fact limit the products and services available to them. In light of this, it may be necessary to consider community expectations and exclude certain entities from participation in the CDR/open banking scheme, where the anticipated negative impacts of greater data sharing (particularly for vulnerable consumers) may outweigh the potential benefits. [↑](#footnote-ref-7)
8. For example, disclosure to non-accredited entities is referred to in [1.26] and [1.47] of the EM. [↑](#footnote-ref-8)
9. See p83-84 of the OB report. [↑](#footnote-ref-9)
10. For example, perhaps the definitions of either ‘accredited data recipient’, ‘data holder’ or ‘CDR data’ (ss 56AF and 56AG) are intended to operate to define the scope of the CDR scheme. However, if this is the case, this is a complex approach, and in our view the boundary is not clearly identified in the legislation. [↑](#footnote-ref-10)
11. The OAIC notes that the reference to only ‘new transaction data’ suggests that, once a consumer becomes a customer, the recipient may need to handle some data in accordance with the Privacy Act (being the ‘new transaction data’), and continue to handle other data in accordance with the privacy safeguards (being information originally obtained under the CDR scheme). The OAIC suggests the implications of this be considered further. [↑](#footnote-ref-11)
12. Note that section 20A of the Privacy Act provides an example of a legislative provision which ‘switches off’ the APPs for credit reporting bodies in relation to certain types of data. [↑](#footnote-ref-12)
13. See EM paragraph [1.168] and [1.169]. [↑](#footnote-ref-13)
14. See s 56BA. [↑](#footnote-ref-14)
15. See the Consumer Data Right Booklet, accessed on 27/8/18 from <https://treasury.gov.au/consumer-data-right/>. [↑](#footnote-ref-15)
16. See s 56EA of the Bill. [↑](#footnote-ref-16)
17. References to de-identified information are also contained in the EM (for example, in paragraphs [1.42] & [1.173]). [↑](#footnote-ref-17)
18. See p 7 of the Consumer Data Right Booklet (available at <https://treasury.gov.au/consumer-data-right/>) which says: *‘**Assistance from the OAIC and external dispute resolution schemes will not be available to large business customers. The ACCC-made rules may provide for other dispute resolution arrangements for them. They will, like all consumers under the system, have access to direct rights of action.’* [↑](#footnote-ref-18)
19. Part V of the Privacy Act applies to ‘interferences with privacy’. [↑](#footnote-ref-19)
20. While certain APPs do include a ‘holds’ requirement (for example, APPs 6 and 7), not all APPs do. [↑](#footnote-ref-20)
21. The Privacy Act only extends to an act done, or practice engaged in, outside Australia by an organisation that has an ‘Australian link’ – see section 5B. [↑](#footnote-ref-21)