Australian Government
Office of the Australian Information Commissioner

Our reference: D2022/007544

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

By email: Kate.ORourke@treasury.gov.au

Re: Consumer Data Right Open Finance (Non-Bank Lending) 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 Open Finance (non-bank lending) 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* (Cth) (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.

My comments are set out in the attachment, and I have provided in this letter a summary of the key issues. 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 Open Finance Sectoral Assessment Consultation Paper (the paper). My recommendations are based on the information available to me at this time.

My key recommendation is that a Privacy Impact Assessment (PIA) should be conducted in relation to the non-bank lending sector as soon as possible. I note the initial PIA for the CDR recommended:

- the PIA be treated as a living document and updated as the legislative framework of the CDR was expanded, and

- the criteria for triggering the need for the PIA to be updated (such as changes which would apply the CDR to another sector, or changes to the scope of data for which the CDR will apply in a particular sector) should be clearly identified.[1]

It is positive to note that Treasury agreed with this recommendation in its response to the initial PIA for the CDR and is committed to carrying out a PIA during the formal sectoral assessment process before a sector is designated for CDR purposes.[2]

The OAIC's guidance on PIAs notes that PIAs are an important component in the protection of privacy, and should be part of the overall risk management and planning processes of APP entities. Undertaking a PIA can assist entities to:

- describe how personal information flows in a project
- analyse the possible impacts on individuals' privacy
- identify and recommend options for avoiding, minimising or mitigating negative privacy impacts
- build privacy considerations into the design of a project
- achieve the project's goals while minimising the negative and enhancing the positive privacy impacts.

While PIAs assess a project's risk of non-compliance with privacy legislation and identify controls to mitigate the risk, a PIA is much more than a simple compliance check. It should '*tell the full story*' of a project from a privacy perspective, going beyond compliance to also consider the broader privacy implications and risks, including whether the planned uses of personal information in the project will be acceptable to the community.

I also make the general observation that further detail and clarity on the proposed datasets and data holders to be designated will need to be provided as part of the formal sector assessment report (required to be prepared under section 56AE), to assist me in considering the privacy impacts as part of my analysis and reporting obligations in the event that section 56AF is invoked.

My comments are set out in detail in the attachment below. They expand on the matters that should be considered in the PIA and address the following consultation questions from the paper from a privacy perspective:

[1] Recommendation 1, *Consumer Data Right PIA,* Maddocks Lawyers, dated November 2019, pp7-8 https://treasury.gov.au/sites/default/files/2019-12/p2019-41016_PIA_final.pdf, accessed 19 April 2022.

[2] See page 17 of Treasury CDR Strategic Assessment Consultation Paper where Treasury notes: '*a Privacy Impact Assessment must be carried out during the formal sectoral assessment process before any sector can be designated for CDR purposes*'; See also Recommendation 1 on page 7 of Treasury CDR Regime PIA (September 2019) and Treasury's response on page 4 of CDR PIA – Agency Response (December 2019).

- Are there privacy concerns specific to non-bank lending that should be taken into account when considering the designation of the sector?
- Do you consider the existing privacy risk mitigation requirements contained in the banking rules and standards are appropriate to manage the privacy impacts of sharing non-bank lending data?
- May the benefits of sharing non-bank lending data vary across particular consumer groups, for example, vulnerable consumers?
- Are there any government-held datasets that would be complementary to privately held datasets and could support possible use cases in non-bank lending?
- If non-bank lending is designated, which entities should be designated as data holders?

Recommendations

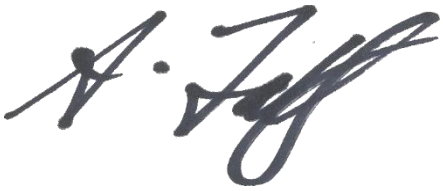
I recommend a PIA be conducted in relation to the non-bank lending (NBL) sector as soon as possible to identify information flows, possible impacts on individuals' privacy, privacy and security risks and to determine if existing risk mitigation strategies are appropriate. Specifically, I recommend this PIA consider:

- the possible impact on the privacy of individuals arising from the different business activities and practices, size and regulatory maturity of entities in the NBL sector
- the possible impact on the privacy of individuals of the proposed de-minimis threshold for the NBL sector and whether entities under the threshold who voluntarily elect to participate in the CDR should be subject to the same privacy obligations that apply to other entities participating in the CDR
- the NBL sector is likely to have a greater number of vulnerable consumers, who may need assistance to provide consent that is fully informed and freely given to the sharing of their consumer data in the CDR
- whether the proposed expansion to the NBL sector raises any risks for the intended interaction of the CDR and credit reporting regimes
- the impact on the privacy of individuals and possible mitigation strategies before designating government datasets for the NBL sector in the CDR.

I also recommend the PIA outline how the agreed upon definition of 'data holder' will impact the various entities listed in the paper, and provides further detail and clarity on the proposed datasets to be designated.

I will consider these matters further as part of any analysis and reporting obligations that may be invoked 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,



Angelene Falk
Australian Information Commissioner
Privacy Commissioner
03 May 2022

OAIC comments on the CDR Sectoral Assessment Open Finance Consultation Paper

Specific privacy risks that could arise in the non-bank lending sector

By way of general comment, I consider that the following contextual factors should be taken into account in relation to the non-bank lending (NBL) sector when reflecting on the effect on the privacy and confidentiality of consumers' information and privacy risks that could arise in that sector:

- the level of privacy regulation
- the level of technological sophistication, privacy and data security awareness and governance maturity, and
- the business models of some NBL entities which could potentially increase privacy risks for vulnerable consumers.

The paper suggests[3] that existing risk mitigation strategies in the CDR Rules and standards will likely be appropriate for managing the risks of sharing NBL data. This suggestion is made on the basis that banking data is already shared in the system, and the same type of data will be shared by non-bank lenders.

However, I would caution against reaching this conclusion in the absence of further analysis. In particular, while the nature of the datasets to be shared may be similar, I note that there are differences in the characteristics of both the data holder and consumer cohorts between the banking and NBL sectors. This may mean there are differences in the likely effect of sharing NBL sector data compared to banking sector data on the privacy and confidentiality of consumers' information. This would suggest differences in the strategies are needed to adequately mitigate any risks that may arise.

Broad cohort, size and regulatory maturity of potential data holders

The paper lists[4] the range of entities within the NBL sector as including payday lenders, cash advance providers and consumer leasing operators. This potential data holder cohort appears to engage in a broader range of activities and practices than the data holder cohort in the banking sector and potentially interacts with consumers who are

[3]See page 17 of the paper: 'Banking data is already shared in the regime and any risks appropriately mitigated in the rules and standards. Any sharing of non-bank lending data (which is likely to be the same type of data as for banking loan accounts) as a result of designation is likely to be appropriately managed through these existing mitigation strategies'.

[4] See pages 11 and 12 of the paper.

unable to access the banking sector. Further, there are a greater proportion of smaller entities in the NBL sector compared to banking.

The potential data holder cohort for NBL is likely to contain a higher proportion of entities that have fewer resources and less capability to comply with regulatory frameworks such as the CDR. The NBL sector may have greater variation in regulatory capability when compared to the banking sector.

The paper notes that many Australian Credit Licence holders (which represents a component of the NBL sector) '*are smaller operators that offer the same lending products but are likely to have lower levels of technological sophistication or data security awareness'*.[5] The paper similarly notes that *'smaller non-bank lenders may not operate at the level required to fully meet CDR obligations in terms of data sharing, customer authentication and information security'*[6]. Further I note that, unlike data holders in the banking sector, it is possible some non-bank lenders are not subject to the *Privacy Act 1988* (Cth)(Privacy Act) and particularly the Australian Privacy Principles, as they may fall within the small business exemption (which generally applies where an entity's annual turnover is less than $3 million).[7]

Where these entities are not covered by the Privacy Act, they do not have obligations to have systems and processes in place to ensure the appropriate handling of personal information. This factor is relevant to their capability to meet data handling-related CDR obligations and could be further heightened if NBL entities are able to participate in the CDR using other pathways that allow for lower levels of accreditation for example through sponsored accreditation. Similarly, while some non-bank lenders may be credit providers under Part IIIA of the Privacy Act, these entities may not be subject to many of the requirements under the credit reporting framework if they are not disclosing information to, or receiving information from, credit reporting bodies.[8] The nature and level of privacy risk arising from designating the NBL sector (which is likely to contain these types of entities) requires further examination.

In recognising this cohort of smaller entities with less regulatory capability exists in the NBL sector, the paper proposes a de minimis threshold be applied to where entities have a customer level small enough to make the marginal cost of compliance with CDR

[5] See page 16 of the paper.

[6] See page 18 of the paper.

[7] See *Privacy Act 1988* (Cth), definitions of 'APP entity' (s 6), 'organisation' (s 6C(1)) and 'small business operator' (s 6D).

[8] An independent review of the Privacy (Credit Reporting) Code 2014 (CR Code) is currently being undertaken. A question being considered as part of this review is whether the CR Code can or should be updated to accommodate other entities and different types of arrangements.

obligations prohibitive for their business.[9] Noting that this threshold has not been implemented in the CDR Rules for the banking sector, this proposal demonstrates that there are differences between the NBL sector and the banking sector. These differences have potential effects on the privacy and confidentiality of consumers and on the risks that apply to this consumer cohort and how they should be managed. This is also contrary to the suggestion in the paper that the impact on the privacy of individuals between these two sectors are similar and can be managed appropriately using the same mitigation strategies as those that exist for the banking sector.

I consider the PIA should assess the business models and practices of some smaller entities within the NBL sector and whether any impacts on the privacy and confidentiality of consumers' information can be appropriately mitigated when designating the NBL sector. I have included these comments below in relation to my discussion about the impacts on vulnerable consumers.

Recommendation 1: the OAIC recommends that a PIA is conducted as soon as possible as part of this sectoral assessment to identify information flows, privacy and security risks of designating the NBL sector and determine if existing risk mitigation strategies are appropriate.

Recommendation 2: the PIA consider the impact on the privacy of individuals arising from the differences in the business activities and practices, size and regulatory maturity of entities in the NBL sector.

Recommendation 3: the PIA assess the possible privacy impacts of the proposal to implement a de-minimis threshold for the NBL sector and whether entities under the threshold who voluntarily elect to participate in the CDR are subject to the same privacy obligations that apply to other entities participating in the CDR.

Interaction between CDR and the credit report system

The interaction between the CDR and the credit reporting system is outlined in s 56EC(3) of the *Competition and Consumer Act 2010* (Cth), which provides that:

> *This Division does not limit Part IIIA (about credit reporting) of the Privacy Act 1988. However, the regulations may declare that in specified circumstances that Part applies in relation to CDR data as if specified provisions of that Part were omitted, modified or varied as specified in the declaration.*

Given the proposed expansion to a broad new cohort of data holders engaging in a wider range of activities and practices, it is important to give careful consideration as to whether

[9] See page 18 of the paper.

this proposed expansion will preserve the intended interaction between the two systems, or whether there is a risk of any unintended consequences arising.

Recommendation 4: the PIA consider whether the proposed expansion to the NBL sector raises any risks for the intended interaction of the CDR and credit reporting regimes.

Impact on vulnerable consumers

Any proposed expansion of the CDR to the NBL sector will require careful consideration of the privacy impact on vulnerable consumers.

The Report arising from the Senate Economics References Committee's Inquiry into credit and financial services targeted at Australians at risk of financial hardship (Committee Report),[10] notes 'real issues' with the business models and business practices of marginal credit service providers such as payday lenders, consumer leases, and debt advice firms.

Page 4 of the Committee Report states:

- *Often these products appear not only to have been targeted at Australians in financial hardship—they seem to have been designed to take advantage of them. It is difficult to escape the conclusion that many providers' business models depend on vulnerable consumers who have limited awareness of other product options, limited negotiating power, and limited propensity to complain about improper or illegal behaviour*.

While it is possible that certain businesses might be excluded from mandatory participation where they fall under any de minimis threshold (and that this might include many of the business models of concern raised in the Committee Report), a PIA would allow a systematic analysis of these business models and practices, associated impacts on individuals' privacy and any privacy risks arising, to inform whether to exclude any particular business or product type[11] or implement additional privacy safeguards in relation to these entities or practices.

Further, as the OAIC has already noted in its submission to the CDR Strategic Assessment Consultation (Strategic Assessment Submission) in September 2021,[12] consumers are not always well-placed to assess the risks and benefits of allowing their data to be shared and analysed in more complex circumstances, and this risk increases with the vulnerability of the consumer. In particular, where vulnerable consumers feel reliant on services or

[10]See Senate Economics References Committee's Inquiry into credit and financial services targeted at Australians at risk of financial hardship.

[11] As contemplated on p 16-17 of the Consultation Paper

[12]See OAIC Submission to Treasury's CDR Strategic Assessment Consultation.

payments, they may feel a loss of control over their personal information and unable to make meaningful choices about the collection, use and disclosure of their data. Where vulnerability is present, it may be appropriate for entities to provide additional resources and support so these individuals can provide informed and meaningful consent.

The above observations demonstrate why the impact on the privacy of individuals needs to be considered afresh (for example, by conducting a PIA), despite the similarities in datasets between the banking and NBL sectors. In particular, when assessing the impact on the privacy of individuals of designating proposed sectors or datasets, it is important to consider whether consent alone provides sufficient protection.

The PIA could consider that the NBL sector is likely to include a greater number of vulnerable consumers, who may need assistance to provide consent that is fully informed and freely given to the sharing of their consumer data in the CDR and examine whether:

- particular NBL products should be excluded from the CDR system, or
- whether more safeguards are required, where:
    - vulnerable individuals need additional resources and support in order to fully understand and provide high quality consent before their CDR data is shared, and/or
    - entities do not have the infrastructure to identify and provide additional support to vulnerable consumers.

Recommendation 5: the OAIC recommends the PIA consider the impact on the privacy of individuals for vulnerable consumers in the NBL sector, with particular consideration given to whether consent adequately mitigates these risks, or whether additional safeguards are required.

Government Data

As noted in the Strategic Assessment Submission,[13] I recommend a cautious approach be adopted if designating government datasets.

Privacy risks are heightened in government-held personal information which is often collected on a compulsory basis e.g. under the Income *Tax Assessment Act 1936* (Cth) or to enable individuals to receive a statutory entitlement or government benefit. Such data is often sensitive and can become sensitive when linked with other datasets. In particular, this may impact vulnerable consumers using the CDR, as their information is more likely

[13]OAIC Submission to Treasury's CDR Strategic Assessment Consultation < https://www.oaic.gov.au/engage-with-us/submissions/OAIC-Submission-to-Treasurys-CDR-Strategic-Assessment-Consultation>.

to be included in such datasets, they may feel reliant on government services or payments and may feel a loss of control over their personal information and unable to make meaningful choices about the collection, use and disclosure of their data. This can call into question whether consent is genuinely informed and voluntary.

Data sets which carry elevated impact on the privacy of individuals should be included only if the privacy impacts are 'reasonable, necessary and proportionate' to achieving the policy objectives of the CDR.

Recommendation 6: That a PIA is conducted to assess the impact on the privacy of individuals and possible mitigation strategies before designating government datasets for the NBL sector in the CDR.

Classes of data for the NBL sector

The paper sets out two categories of possible NBL datasets that may be designated to be available under the CDR on page 14: consumer data and product data. I note the descriptions of each class of data provided on page 14 are not exhaustive and the proposed consumer datasets for designation are not settled at this stage.

While page 14 of the paper suggests that rules and standards applying to the NBL leverage those that currently apply to the banking sector,[14] page 15 acknowledges that there may be different products and datasets in this sector. The impact on the privacy of individuals associated with designating these datasets, and appropriate mitigation strategies, need to be considered before these datasets are designated. For example, consideration of whether certain products or datasets could reveal insights about the financial capacity of a vulnerable consumer and influence the goods or services that are subsequently offered to the consumer.

Further detail and clarity provided as part of the formal sector assessment report published under section 56AE, will assist me in considering the privacy impacts more fulsomely as part of any analysis and reporting obligations if section 56AF is invoked.

Designation of data holders in the NBL sector

As indicated by the question on pages 11 and 16 of the paper, I note that Treasury is still considering how data holders will be defined and that two statutory definitions are under consideration: 'credit facility' in the *Australian Securities and Investments Commission Act 2001* (Cth), and 'registrable corporation' in the *Financial Sector (Collection of Data) Act 2011* (Cth). I will consider further detail provided in any draft designation instrument and

[14] Page 14 of the paper.

explanatory statement to clarify how the proposed definition will apply to entities in the NBL sector. This additional information will assist assessment of the privacy impacts of this sector and, together with the information provided by a PIA, will help inform whether certain business types or product types ought to be excluded, or whether additional safeguards to protect consumers' privacy can be introduced.