Financial Rights LEGAL CENTRE

Submission by the Financial Rights Legal Centre

Treasury

Consumer Data Right, Privacy Impact Assessment, December 2018

January 2019

Financial Rights Legal Centre |PO BOX 538, Surry Hills 2010 | Tel (02) 9212 4216 |Fax (02) 9212 4711 | info@financialrights.org.au | www.financialrights.org.au | @Fin_Rights_CLC | ABN: 40 506 635 273

About the Financial Rights Legal Centre

The Financial Rights Legal Centre is a community legal centre that specialises in helping consumers understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers. We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues. Financial Rights operates the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies, and the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters. Financial Rights took close to 25,000 calls for advice or assistance during the 2017/2018 financial year.

Financial Rights also conducts research and collects data from our extensive contact with consumers and the legal consumer protection framework to lobby for changes to law and industry practice for the benefit of consumers. We also provide extensive web-based resources, other education resources, workshops, presentations and media comment.

This submission is an example of how CLCs utilise the expertise gained from their client work and help give voice to their clients' experiences to contribute to improving laws and legal processes and prevent some problems from arising altogether.

For Financial Rights Legal Centre submissions and publications go to
www.financialrights.org.au/submission/ or www.financialrights.org.au/publication/

Or sign up to our E-flyer at www.financialrights.org.au

National Debt Helpline 1800 007 007
Insurance Law Service 1300 663 464
Mob Strong Debt Help 1800 808 488

Monday – Friday 9.30am-4.30pm

Introduction

Thank you for the opportunity to comment on Treasury's Consumer Data Right Privacy Impact Assessment (**PIA**).

Financial Rights Legal Centre (**Financial Rights**) supports the addition into the PIA of a number of recommended elements including:

- consideration of vulnerable and disadvantaged consumers;
- increased consumer testing;
- increased information regarding the impacts of access to CDR by non-accredited data; and,
- explanations of why certain mitigants raised by consumer representatives have been rejected.

These are positive steps in more fully considering the impacts of the Consumer Data Right (**CDR**) upon privacy.

However Financial Rights continues to have concerns with both the approach taken by Treasury in undertaking this assessment and with some of the substance of the assessment itself. These issues are discussed below.

Conduct of the PIA

We note that the Treasury have decided not to outsource the development of the PIA to external consultants. We remain disappointed in this decision.

While we acknowledge there is no strict requirement for Treasury to have undertaken an independent assessment, we believe that the approach taken to undertake the PIA is flawed, conflicted in nature and not in keeping with the recommendations of the OAIC in its Privacy Impact Assessment guidelines.

We note that Treasury explains the decision to undertake the PIA internally in a number of ways.

First, the PIA states:

> *The CDR regime as a whole is largely directed at protecting the data of consumers, including individual's data. It was therefore not appropriate to separate the assessment of privacy impacts and proposals to address privacy risks from the core policy development function being undertaken by Treasury.*

We acknowledge that it is clearly the case that Treasury have a policy development function in implementing the CDR regime. In implementing and developing this policy though there is a fundamental balancing act that needs to take place between the

protection of personal information of Australians with the interests of business in carrying on or innovating their profit driven activities. The regime being proposed is therefore not solely directed at protecting the data of consumers– it is directed at balancing the specific interests of consumers in accessing their own data with the specific interests of business to innovate and create new business models based on the use of that data. This economic element has always been an integral part of the data bargain, and remains a key underlying assumption to its implementation. As the Productivity Commission stated in its Inquiry into Data Availability and Use Report:

> *Effective use of data is increasingly integral to the efficient functioning of the economy. Improved availability of reliable data, combined with the tools to use it, is creating new economic opportunities. Increasing availability of data can facilitate development of new products and services, enhance consumer and business outcomes, better inform decision making and policy development, and facilitate greater efficiency and innovation in the economy.*[1]

We also note that this economic element is downplayed in the PIA, with benefits to privacy highlighted. The Objectives of the Consumer Data Right section states:

> *It is partially intended to enable the development of third party services that may enhance privacy rights, by helping individuals to understand what data is held by businesses and understand and manage collection, use and disclosure permissions.*[2]

The use of the word partially, in our view, understates the case. The creation of new FinTech services is a fundamental part of the CDR, without which it would not even be viable. The object of the Act is to create more choice and competition,[3] the only way this can occur is if there are new FinTech services to assist people to do compare.

The policy development process in implementing the CDR can therefore lead to greater or lower privacy protections depending where this balance is judged to be. It is for this reason that the privacy impact assessment should be completed by an independent body. The OAIC guidelines state that:

> *Some projects will have substantially more privacy impact than others. A robust and independent PIA conducted by external assessors may be preferable in those instances. This independent assessment may also help the organisation to develop community trust in the PIA findings and the project's intent. Footnote: A number of privacy consultancies and law firms offer PIAs as a service.*[4]

The decision not to in this case gives rise to a possible perceived or actual conflict of interest. Given Treasury's mandate by government to implement a Consumer Data Right in a very short period, it could be seen to be in Treasury's interest to downplay any privacy

---

[1] Page v. Productivity Commission, Inquiry into Data Availability and Use Report, https://www.pc.gov.au/inquiries/completed/data-access/report/data-access-overview.pdf

[2] Page 18, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[3] Section 56AA(c) *Treasury Laws Amendment (Consumer Data Right) Bill 2018*

[4] Page 10, Office of the Australian Information Commissioner, Guide to undertaking privacy impact assessments https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf

issues that may arise from consideration of the CDR and therefore delay the implementation. A poor *independent* privacy impact assessment may, for example, recommend a re-think of the legislation to bolster privacy protections, which may have obvious policy development implications. The current assessment in our view does downplay many risks. This will ultimately go to undermining community trust in the CDR and the Government's role in implementing it. Given increasing community concerns with respect to Government data initiatives such as the My Health Record and the most recent Census, this lack of trust is likely to be considerable – especially when the first sign of problems arise.

Second, the PIA states:

> *This development process took place over approximately 18 months, in an iterative way, involving multiple consultations. This did not lend itself to a point in time assessment by external consultants.*[5]

Any point in time along this process – particularly after the exposure draft bill was developed could have been an appropriate time to begin. Given the delay in the implementation timeframe, now would be a good time too.

Third, the PIA states:

> *The internal development of the PIA also reflects Treasury's recognition of the importance of developing internal capability in relation to PIAs and a better understanding of the privacy issues and risks raised by the CDR as part of its design. This was a secondary factor in the decision to conduct the PIA internally and had little influence on the decision.*[6]

Using the development and implementation of legislation that will have a profound impact upon Australian's privacy as a training ground for PIA capabilities seems inappropriate. If there is any case that requires experience and expertise it would be this one.

As we understand it, Treasury's consideration of many of the privacy risks was limited to internal brainstorming sessions with no specific external consultations or surveys. Without specific privacy expertise, nor expertise in the behaviours of the financial services sector and the burgeoning FinTech and IT sectors that external, independent perspectives could provide, we believe the approach taken is flawed.

Finally, given OAIC's role in the CDR, the decision by Treasury to go against the explicit advice of the co-regulator is problematic and does not provide any more confidence in the process or the OAIC advice.

Recommendation

1. **Treasury should engage an external consultant to finalise the development of the current PIA.**

[5] Page 30, Treasury, Consumer Data Right, Privacy Impact Assessment, December 2018

[6] Page 30, Treasury, Consumer Data Right, Privacy Impact Assessment, December 2018

Mapping of personal information flows

The PIA attempts to describe the personal information flow using the example of Naomi.[7] While this describes the complexity of the data flow and is somewhat useful – what remains missing is a description of what privacy protections will be available to a consumer at every step of this flow.

The complexity of what is being proposed with respect to the application of APPs, CDR Privacy protections and general law at different stages remains obscure and difficult for industry, lawyers, and consumer representatives to understand, let alone a consumer.

An explanation, flowchart or visualisation of what privacy protections apply at what stage should be a central feature of the Privacy Impact Assessment. Understanding what protections are available when and applying to whom would be in our view critical for a comprehensive privacy assessment to be undertaken. Without it, the privacy assessment is incomplete.

Consumers need to be aware of their privacy rights at different stages of the process in order to build confidence in the CDR. This is because there are higher and lower levels of protection at different stages and the level of protection should influence their decision making process. Simply asserting that consumers can simply complain to External Dispute Resolution (**EDR**) after the fact and find out what protections apply is inadequate and fundamentally undermines the stated aim that consumers be educated in their consumer data rights.

If it is too complicated for Treasury to create a simple explanation it will be too complicated for consumers to understand.

Recommendation

2. **An explanation, flowchart or visualisation of what privacy protections apply at what stage should be included in the Privacy Impact Assessment.**

[7] Stages 1-6 at Pages 41-42, Consumer Data Right Privacy Impact Assessment.

Vulnerable and Disadvantaged Individuals

Financial Rights commends Treasury on the inclusion of a section on vulnerable and disadvantaged individuals and the inclusion of vulnerability considerations in Recommendations 1 and 3.

We wish to make one comment though. Further categories of vulnerability and disadvantage should be listed explicitly in this section, including:

- People suffering from mental health issues
- Older Australians
- Aboriginal and Torres Strait Islander peoples

While the first two groups have been appropriately mentioned in the consent section, this is not enough. These groups have unique experiences and issues that will mean the CDR will impact upon them in different ways and they will experience Open Banking and their Consumer Data Rights in ways very different to other Australians.

Recommendation

3. **People suffering from mental health issues, Older Australians, Aboriginal and Torres Strait Islander peoples should be explicitly listed in the section addressing Vulnerable and Disadvantaged Individuals.**

Mitigants that were not adopted

Banning other forms of sharing of CDR data

We note that the PIA raises the issue of screen scraping. In part the PIA states:

> *There are a broad range of data sharing arrangements currently in place. The CDR regime cannot meet all of the different tailored requirements of these arrangements. Prohibiting them would have significant negative impacts on consumers and business. As the CDR develops it is expected that it will meet the needs of many of these arrangements. If the CDR is designed and implemented in a way that is efficient, convenient and that inspires confidence in consumers and businesses, it is expected that consumers and business will choose to use the 'safe pipe' that it represents.*

The position that if there is a safer more trusted option then consumers will use this service rather than the unsafe service, fundamentally misunderstands both the incentives of bad

financial services actors to avoid the safe pipes altogether, and the real world incentives for consumers to submit to these bad actors and use the unsafe pipes.

A number of points need to be made. Firstly, the higher regulatory hurdles of CDR accreditation will be a significant disincentive for these businesses, particularly fringe financial services, from joining.

Second, financially vulnerable people will continue to be desperate enough to seek fringe financial services and will do anything, including signing up to a service that uses unsafe screen-scraping practices in order to gain access to these services. Many of these consumers will not concern themselves with the nuances of privacy protections to do so. If it means engaging with and submitting to the requests or demands of non-CDR accredited entities like pay day loan operators or other emergent services, financially vulnerable consumers will do so. This will result in financially vulnerable people ending up with lower privacy protections and at greater risk to harm due to lack of protection from existing protections. For example, accessing data via 'screen scraping' technology amounts to a breach of the terms and conditions of a customer's bank account, as the consumer is handing over their PIN or access to their online account. If they were then to have funds taken from their account the customers is at risk of losing their protections under the E-Payments Code as they have, by allowing access to a third to their account[8]

The PIA does not address the outcomes from this inevitable regulatory arbitrage. While the CDR Bill includes the offences of misleading or deceiving a CDR consumer and holding out as an accredited person, it does not address the situation where the consumer is pressured to provide the CDR data to an entity using screen scraping technology who is clearly stating that they are not an accredited entity, whereby gaining inappropriate access to the consumer's CDR data. This remains the case, despite the new ACCC rules preventing the sharing of CDR data with a non-accredited entity in version one of the Rules.[9] This is because consumers will be able to still access their own data and pass this on to the non-accredited entity in a form that they will be able to use.

We note again that screen-scraping has been banned in other countries such as the UK.

Recommendation

4. The PIA needs to address the issue of screen-scraping and makes recommendations that mitigate the problems that arise from its interaction with the CDR regime.

[8] See discussion in the Final Report of the Small Amount Credit Contract Review, March 2016, at p. 76-77, available at https://static.treasury.gov.au/uploads/sites/1/2017/06/C2016-016_SACC-Final-Report.pdf.

[9] Rule 8.8, ACCC CDR Rules Outline, December 2018,

Other possible mitigants as yet unconsidered.

Financial Rights has previously put forward risk mitigation strategies for some of the privacy risks that arise. Many of these have now been considered in the PIA. However others have yet to be addressed and we believe need to be. While we accept that they may be rejected we believe Treasury needs to specifically and explicitly explain why these obvious risk mitigation strategies have been rejected. These include:

- A legislated prohibition of on-selling as opposed to leaving this to the ACCC rules;
- An outcomes-based regulatory approach that could include post-purchase/post-initiation audit surveys to find out what consumers believe that they have consented to and whether this aligns with the consents as formulated by the data recipient. These audits would be compulsory, conducted independently and require a certain percentage of consumers to have understood the consents, otherwise, data recipients will need to improve their consent and have increased monitoring to ensure their consent process meets best practice. Such an approach will give industry the ability to innovate, while ensuring that they meet regulatory expectations.
- The use of RegTech to develop market analyses of CDR products and services to examine actual consumer outcomes in the finance services market. Regulators should be provided with detailed market monitoring tools with transaction detail data for everything from default data, claims, sales and quotes data to transaction information;
- Introducing concepts of anonymised data (where re-identification is impossible by any party by any means) and pseudonymous data (except re-identification techniques are reasonably likely to be used) be embedded in the Consumer Data Right and the Open Banking regime.
- Strengthening of CDR privacy protections as recommended in our previous submission

Recommendation

5. **The PIA needs to address a number of mitigation strategies put forward by consumer representatives including:**
   a) **a legislated prohibition of on-selling data;**
   b) **the introduction of an outcomes-based regulatory approach that includes post-purchase/post-initiation audit surveys;**
   c) **the use of RegTech to develop market analyses of CDR products and services to examine actual consumer outcomes;**

d) **introducing concepts of anonymised data and pseudonymous data to improve controls over the subsequent use of data;**

e) **further strengthening CDR privacy protections.**

Risk Rating Matrix

The Risk Rating Matrix as presented in the PIA is problematic. The risk severity is as we understand determined by the typical case rather than the extreme case.

This leads to the strange outcome seen at Scenario 2.1[10] where the example provided regarding political views is leaked, the likelihood of that leaking happening as highly likely and the risk severity is deemed minor. Political views are one of the categories of sensitivity under the *Privacy Act*. The breach and misuse of political views drawn from data farming on Facebook has arguably led to major impacts upon western democracy. This is not a minor privacy breach for either the individual or society as a whole.

It also leads to similarly absurd outcomes at Scenario 1.3, which states:

> *The individual may engage an accredited data recipient who instead seeks data outside the CDR system. E.g. Naomi may engage with a tech company believing that access is obtained through the regulated framework of the CDR. The data recipient instead obtains her personal information through screen scraping.*[11]

The risk severity here is deemed "minor" despite the fact that screen-scraping takes away all the persons rights under the terms and conditions of the data-holder and can involve severe subsequent problems (see above on page 8).

Scenario 4.5 states:

> *The data holder may intentionally or unintentionally send inaccurate data. E.g. NN Bank sends transaction data to BetterDeals containing transactions processed by NN Bank in error.*[12]

This is however deemed a minor severity despite the fact that the wrong details will feed into algorithms producing significant flow on impacts upon an individual's credit worthiness, credit ratings or be prevented from accessing certain services at all. This is not a minor consequence for most people.

By developing a risk severity rating based upon a probability distribution ensures that the severe consequences that impact upon an individual will be nullified by the breadth of the population or reference to a typical case.

[10] Page 55, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[11] Page 54, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[12] Page 60, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

We recommend that if Treasury are stuck with the format, at the very least for each Potential Risk that at least 5 examples be provided – extreme, major, moderate, minor and insignificant scenarios. An extreme example leads to extreme outcomes, a minor risk, minor outcomes. It is misleading to present a generalised description of severity given the multiplicity of cases.

We recommend too that a full description of the process Treasury undertook to determine risk severity be included in the PIA for transparency's sake and for the public to better understand how Treasury came up with the determination.

Subsequently we recommend that Treasury consult widely on risk severity. While we are sure Treasury is diverse there is no way Treasury employees could be in any way seen to be representative of the broader community and they can not reflect general attitudes towards privacy matters.

Recommendation

6. **Treasury should reconsider the use of the risk matrix and consult widely on risk severity of the scenarios listed.**

Treasury judgements as to likelihood

As with risk severity, we do not agree with many of the judgements made by Treasury with respect to the likelihood of a risk.

For example scenario 4.10 is deemed "unlikely":

> *A third person may pose as the accredited data recipient to gain access to the individual's raw transaction data from the data holder. E.g. A third person could pose as BetterDeals to request and obtain Naomi's raw transaction data from her bank, NN Bank.*[13]

This however is highly likely in a great number of scenarios including many in-store sales scenarios, in scenarios involving aged parents and their children, with parents and their young children; as well as non-English speaking consumers and their English speaking relatives.

Scenario 5.2 states

> *The accredited data recipient may misuse the information provided by the individual in a way technically consistent with their authorisations. E.g. BetterDeals may use information such as emails, telephone numbers, and other personal details in a way that, while technically consistent with an authorisation, is improper or abusive.*[14]

This is deemed "possible" by Treasury. It is our expectation that data collector's will regularly seek to use data that may be technically consistent with consent but are used in

[13] Page 61, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[14] Page 61, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

ways not necessarily understood by the consumer or not conceived of by the consumer. This use (or misuse) of data seems to us to be the entire business model of data harvesters.

Recommendation

7. **Treasury should reconsider the likelihood ratings and consult widely on the likelihood of the scenarios listed.**

Additional Consumer Data Right Scenarios – Risk Assessment

Non-accredited parties

We note that the PIA states, in part:

> *The CDR does not create rights for consumers to direct accredited entities (or original data holders) to transfer their data to non-accredited entities. It may allow accredited persons to voluntarily do so at the direction of the consumer. Therefore the potential is limited for non-accredited entities to pressure individuals to provide their personal information outside of CDR frameworks as a condition of receiving a service.*[15]

While the CDR does not create rights for consumers to direct accredited entities (or original data holders) to transfer their data to non-accredited entities, consumers do have the ability to request their own data and this can be in a format that could be read by a computer program – whether it is in a pdf or other machine readable or screen scrapable format. It is this ability that enables non-accredited entities to potentially pressure individual consumers to provide the personal information outside of the CDR regime - not necessarily the consumer's direction to an accredited party.

This issue is actually raised later under the *Preventing the consumer from accessing their own data* section[16]. The PIA states:

> *Some stakeholders have raised concerns that if consumers have the right to access their own data, with the data provided in a useable form, unscrupulous actors will use the consumer to bypass the accreditation requirement.*
>
> *It has been suggested that this skirting of the CDR framework could be achieved, for example, by the third party not receiving the data themselves but instead providing the consumer with the software that enables the consumer to download the data via an API.*

[15] Page 66, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[16] Page 100, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

> *CDR data would then be stored on the consumer's device or on cloud storage under an account that is owned by the consumer, but accessed by the non-accredited third party.*[17]

This still does not quite capture the concern described above but gets close.

In rejecting a closed system, the PIA suggests that there will be risk mitigants available. The PIA suggests that:

> *this risk could be mitigated by ensuring data holders are not required to provide this access through an API in standardised formats. Data holders could instead be enabled to determine the format in which this information is provided to the consumer, so long as it is provided in a user-friendly digital format.*[18]

A user-friendly digital format is easily "screen scrapable" to gain access to the consumer data – again, a process not prohibited under the CDR regime.

The PIA goes on to state:

> *Greater friction would be introduced if the consumer accessed this information themselves rather than disclosing it to an accredited person.*[19]

This friction may exist but given the opportunities and incentives involved in a particular transaction with a desperate consumer, facing financial hardship and a bad actor financial services entity, this friction is a minor hurdle and easily overcome.

Then the PIA states:

> *Additionally, education and clear branding of CDR transfers would ensure consumers know that when they are transferring this way, they are no longer using the CDR (see below for further discussion of branding).*[20]

While helpful, a desperate consumer, facing financial hardship will be willing to ignore all advice.

Finally the PIA states:

> *While this would not prevent consumers being used as a funnel in every instance, and as such would not eliminate this risk, it would act as a de facto barrier for the majority of consumers who are considering sharing their data with a non-accredited third party.* [21]

Ultimately we agree with Treasury on this point. It may very well prevent most people from engaging in risky behaviour but it will be the vulnerable consumer, the consumer experiencing financial hardship that will be most at risk under the CDR regime as currently designed.

---

[17] Page 110, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[18] Page 110, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[19] Page 111, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[20] Page 111, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[21] Page 111, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

Treasury Privacy Recommendations

Recommendation 1 - Behavioural research

Financial Rights supports the proposal to have the Data Standards Body to have regard to vulnerable groups and that

> *Test groups should be of sufficient size and diversity to provide justified confidence in the safety of consent processes.*[22]

We note that

> *Initial research will be undertaken in three stages. There will be at least 20 participants in the first stage, a further 50 in the second stage, and a further 20 in the third stage. Participants will be recruited by CHOICE. It is expected that further research will be undertaken throughout the implementation of the CDR*

We are not entirely confident that the full range of vulnerabilities will be able to be represented in a sample size of 90 and consideration should be given to increasing this sample size as appropriate. While we presume they will be, we recommend the full results of these tests be made public.

Recommendation 4 – preventing undue weight on the benefits of competition and innovation

Financial Rights supports this recommendation except that it is incredibly vague. What defines undue weight? When will we know undue weight has been given by a regulator on competition issues? It is a subjective test that will provide the opportunity to claim that they did not provide undue weight to these factors. It needs to be further defined and should be quantified.

Recommendation 7 – consumer education

We recommend that any education about the CDR should be less a sales pitch for the benefits of open banking and open data generally but specifically raising awareness about the risks and provide warnings to consumers of the potential negative consequences of breaches etc.

Recommendations

8. **Treasury should consider resourcing an increase to the sample size in consumer testing to ensure that appropriate levels are reached**

[22] Page 117, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

9. **The consumer testing results should be made public.**
10. **Further guidance on the meaning of undue weight should be provided.**
11. **Education about the CDR should focus on raising awareness about the risks of the sharing of data and provide warnings to consumers of the potential negative consequences of breaches.**

Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact Financial Rights on (02) 9212 4216.

Kind Regards,

Karen Cox
Coordinator
Financial Rights Legal Centre
Direct: (02) 8204 1340
E-mail: Karen.Cox@financialrights.org.au