Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

1 March 2019

Senate Standing Committee on Economics
PO Box 6100
Parliament House
Canberra ACT 2600

By email: economics.sen@aph.gov.au

RE: Inquiry into Treasury Laws Amendment (Consumer Data Right) Bill 2019

This submission from the Australian Privacy Foundation (The "APF") responds to the inquiry into the Treasury Laws Amendment (Consumer Data Right) Bill 2019 (the "CDR Bill"). It is noted that we received a letter about this inquiry on 20 February 2019. Submissions were due on 28 February 2019. This left just 8 days to prepare a response. This is inadequate time to give a considered response. As a consequence, our comments are brief.

Introduction

The Foundation strongly supports the rights of people to have control over their personal information. The Consumer Data Right (CDR) is supporting and facilitating this pre-existing right. The Foundation, in principle, supports the CDR. It is essential that all Australians have strong privacy safeguards in place so they can use the CDR with trust and confidence.

The success of 'open banking' or the CDR will depend heavily on gaining the trust and confidence of Australians in the system, and this in turn will only be well founded if such trust and confidence is based on a scheme that is trustworthy (worthy of trust). People need to be certain that the risks are well understood and acknowledged, and that their data will be collected minimally, stored securely (both against unintended re-identification and the inevitable hacking), used as requested, not exposed to coerced or widespread distribution, deleted on demand or as soon as practicable, and that the risks that will grow over time are not merely projected on defenceless data subjects but are pushed back on the proponents, so there are consequences (including fines and compensation, which the subject can take legal action to pursue) for misuse or foreseeable neglect.

As outlined below, we consider the framework as it currently stands unnecessarily exposes people to harm because the fundamental privacy safeguards are not in place and risks have been severely underestimated by the Government. These issues can be rectified by ensuring that an external rigorous and independent Privacy Impact Assessment is performed with the implementation of the recommendations from this assessment. This is a first necessary step and as new risks become apparent there needs to be a process to ensure those risks are managed. If the legislation is enacted without this process, Australians are left at a higher risk of harm.

Rushing through the CDR

We remain concerned that the move to introduce CDR is simply too fast. The consultations and the sheer amount of information to look at has meant that the consultation process is not working effectively. We agree with the announced delay and the decision to pilot the system.[1]

It is unclear why there is a rush. The equivalent system in the United Kingdom has had a very slow take up and has not delivered any competition or financial revolution to date.[2] This should be expected as trust needs to be built over time.

The introduction of the CDR Bill into Parliament is yet another rushed process. We strongly recommend that the Committee have further time to consider the complex issues in this matter so a detailed list of issues to be considered can be made.

Australians do not have adequate privacy protections in place

The Foundation repeatedly writes submissions highlighting the major problem that we do not have adequate privacy protections in Australia. The privacy protections for Australians are vastly inferior then those in Europe and the UK. For example, in the UK people have the following privacy protections:

1. UK has adopted and complies with the *General Data Protection Regulation* (GDPR);
2. UK has a *Human Rights Act*; and
3. UK has an adequately-funded, active privacy regulator

This means that whatever legislation is introduced is built on an inadequate foundation. Further data sharing increases the risk of harm.

Recommendations:

Australians need adequate privacy safeguards to ensure they can use the CDR with trust and confidence. The key protections needed are:

-Privacy laws that are benchmarked to (or exceed) the protections in the GDPR
-A *Human Rights Act*
-Adequately funded, active and tough privacy regulator

[1] See https://www.innovationaus.com/2019/01/Open-banking-quietly-delayed.
[2] See https://www.raconteur.net/finance/open-banking-moving-slowly

Regulators – ACCC and OAIC

Privacy safeguards and the success of the CDR depend on strong regulators. The ACCC is a strong regulator. Unfortunately, the OAIC is not a very active regulator and appears to be severely under resourced. The culture of the OAIC seems to be "soft" and it has sent a clear signal to industry that there is very little chance they will ever be fined or sanctioned over data breaches. The Government must ensure that the OAIC is adequately funded, has greater powers and is tough on privacy breaches.

Fines and civil penalties

The Final Report of the Financial Services Royal Commission should be considered in the context of the CDR Bill. The Royal Commission established that "enforceable undertakings" and small penalties did not stop poor behaviour. Both regulators must have powers to impose significant fines for data breaches by a CDR Participant. Data breaches should also start a process for removal of accreditation.

CDR Rules

The structure of the CDR framework is to have a framework of binding Rules with the legislation as an anchor for that detail. In our view, the Rules obtain the most critical detail to protect people from harm and Members of Parliament need to consider that information. The Rules framework is also incredibly complex and difficult to understand. The legislation is only a high-level framework. This Inquiry is only considering the legislation and not the Rules. We argue this is a mistake. Both the Rules and the CDR Bill need to be read together and considered by Parliament to ensure the package works as a whole.

Robust consumer testing is also critical to ensure that the CDR actually works for consumers.

Recommendations:

Members of Parliament need to consider the Rules and the CDR Bill to ensure it is appropriate.

Robust consumer testing must be completed before implementing the CDR for any sector.

Access to justice

The CDR Bill does contain a section on accrediting External Dispute Resolution Schemes (EDR). There is no section that contains clear rights for consumers to access orders and compensation (both financial and non-financial) in both EDR, the OAIC and Court. People need to have a range of rights to injunctions, deletion of data, rectification orders and compensation. This must be in the legislation so people have access to justice. The current laws in the Privacy Act are inadequate and this is demonstrated by the very few decisions of the Privacy Commissioner. It is also unclear whether EDR will deliver adequate consumer redress given the particular limitations of those schemes.

In summary, the current process for raising a dispute about a privacy breach with the OAIC is inadequate. The OAIC makes very few decisions, awards very little compensation, has a short

time limit of 12 months and discontinues investigation of the majority of complaints made. All of these problems must be rectified.

EDR needs to have clear powers to consider CDR disputes for each scheme, be required to consider those disputes and be able to award adequate compensation for both financial and non-financial loss. For example, non-financial loss in AFCA is limited to $5000.

Recommendations:

Access to dispute resolution in the OAIC needs significant improvement including a time limit of 6 years, a requirement to investigate and determine complaints and award compensation (both financial and non-financial) that is adequate.

EDR schemes recognised for CDR must have the ability to consider CDR disputes, award adequate compensation (both financial and non-financial).

Bundled consent – Data must be given to get a service

We remain concerned that people will be told that in order to access a service they will be required to sign consents for the service provider to get their data from a range of other services. Unfortunately, consumers are used to this as it happens frequently. The CDR Rules attempt to stop this but we consider that this risk remains highly likely. Consumer testing could assist but further work is required to protect people from harm. As detailed below a rigorous external PIA process would assist in getting an effective approach to tackle this problem.

Privacy Impact Assessment (PIA)

The Privacy Impact Assessment process and the draft document released by Treasury do not meet the standards required of competency, transparency and fairness.

Treasury first informed consumer advocate stakeholders about the PIA in November 2018. The PIA had been internally prepared by Treasury. The OAIC PIA Guide[3] recommends that a specific PIA process should be integrated from the beginning of the process. [4] This did not occur. The OAIC PIA Guide also recommends that for projects with significant privacy impacts that a "*robust and independent PIA conducted by external assessors may be preferable*." [5] The PIA was prepared internally by Treasury and there is no evidence that Treasury has the expertise for this process.

Treasury then released the PIA for consultation on 21 December 2018 with submissions due on 18 January 2019. This was an attempt to hide the consultation in the holiday season so no one would notice. The Foundation put in a submission. As of today, **no submissions have been published following that consultation.** This is a failure of transparency and fairness.

[3] Guide to undertaking privacy impact assessments, Office of the Australian Information Commissioner, May 2014 available at https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.

[4] See Page 3 OAIC PIA Guide "To be effective, a PIA should be an integral part of the project planning process, not an afterthought."

[5] Page 10 OAIC PIA Guide.

The Australian Banking Association did publish their submission to this consultation on their own website.[6] The Foundation has read their submission and shares their concerns. A particular concern we share is the assessment of privacy risks in the PIA are very unrealistic. A particular concern is the third-party misuse of data. This is rated as "unlikely" when we would argue it is highly likely. An enormous risk for consumers is that small third-party companies will appear to offer deals and get data and then simply disappear and sell or move the data. In summary, the PIA and the current Rules and Legislation Framework has not properly planned for a likely risk. This is a serious oversight.

The PIA (as currently drafted) is inadequate and leaves people significantly exposed to harm. The privacy protections in Australia are far weaker than the UK and greater care needs to be taken in Australia to protect people. A failed PIA process means we do not even know what is missing. A rigorous, credible and external PIA process gives a wide range of stakeholders the ability to identify risks, realistically assess those risks and introduce protections. None of this has occurred.

The Government then introduced the CDR Bill into the House of Representatives on 13 February 2019 even though there were serious concerns about the PIA from at least two stakeholders. None of those concerns have been resolved.

Recommendations:

The Government arrange to appoint an independent and credible external organisation with significant expertise in PIAs to conduct a PIA for the 'Consumer Data Right'.

The legislative process is delayed to ensure that adequate privacy safeguards are in place.

If you have any questions please do not hesitate to contact Kat Lane.

Yours sincerely

Kat Lane
Vice-Chair
For the Australian Privacy Foundation Board
0447 620 694
Kat.Lane@privacy.org.au

[6] The submission is available at https://www.ausbanking.org.au/images/uploads/PIA_CDR.pdf.