Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

10 May 2019

ACCC
Consumer Data Right draft rules consultation

Uploaded via ACCC Consultation Hub

RE: CDR Draft Rules

This submission from the Australian Privacy Foundation (The "APF") responds to the Exposure draft 29 March 2019 *Competition and Consumer (Consumer Data) Rules* 2019 (the "CDR Rules").

Introduction

The Foundation strongly supports the rights of people to have control over their personal information, including access to it and influence over how it is used (already codified in the Australian Privacy Principles, particularly APP 12). The proposed 'Consumer Data Right' (CDR) is justified in part on the basis that it supports and facilitates this pre-existing right. The Foundation, in principle, supports the CDR to the extent that it effectively supports this control. Concerns about it focus on the degree to which the capacity to direct where and how personal data is provided and disclosed to other entities becomes a de facto obligation to do so, which would undermine actual control.

It is essential that Australians have strong privacy safeguards in place so they can use the CDR with trust and confidence.

The success of the proposed 'open banking' regime and 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 of taking advantage of the CDR 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, and deleted on demand or as soon as practicable; and that

- the risks in the CDR model 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 effective fines and adequate compensation, which the subject can take legal action to pursue) for misuse or foreseeable neglect.

Those concerns are consistent with a substantial body of case law, with the principles evident in the *Competition & Consumer Act 2010* (Cth) and with effective enforcement by benchmark regulators such as the Australian Competition & Consumer Commission. (We note that the Commission has recurrently highlighted the need for effective regulation under the Act and has accordingly recurrently called for stronger penalties on the basis that current policy settings inadequately deter corporate wrongdoing.)

The decision to not include a "right to delete" data, as expected and promised through the consultation process, is a major failure for consumer protection, and a fundamental flaw in the scheme. The lack of a right to delete appears to be positive proof that the CDR is designed with business interests at top of mind mind, and not for consumers. The right to delete must be drafted comprehensively into the CDR Rules as a matter of urgency. Any decision not to include this right means that the CDR is not a 'right', it is a failure -- a failure that will not benefit consumers, that will lead to deserved distrust, and that will stymie the competition benefits sought by the Productivity Commission and Treasury.

We remain very concerned that the framework as it currently stands unnecessarily exposes people to harm because the fundamental privacy safeguards are not in place in Australia, and the risks around 'open data' and about 'voluntary' data disclosure practices that may become obligatory in commercial practice have been severely underestimated by the Government.

It is essential that all of the issues in this submission are comprehensively addressed before proceeding further.

Part A – Overall comments

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
4. UK courts have appropriately recognised the importance of privacy in a wide range of circumstances and have exercised their authority to deter wrongdoing

Systemic deficiencies in the Australian regime at the Commonwealth and state/territory levels mean that whatever CDR legislation is introduced is built on an inadequate foundation. Further data sharing increases the risk of harm.

Recommendation 1

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, including a right to sue for breach of privacy as long recommended
- A *Human Rights Act*
- Adequately funded, active and tough privacy regulator

Fundamental problems still not addressed

External Privacy Impact Assessment

There must be an external rigorous and independent Privacy Impact Assessment (PIA) with the implementation of the recommendations from this assessment legislated in both the CDR legislation and rules. This step has never happened. The PIA was drafted internally by Treasury and numerous concerns from a wide range of parties have been ignored. The PIA by Treasury does not comply with the *Guide to undertaking privacy impact assessments* issued by the OAIC.[1] The OAIC also suggested that Treasury give "serious consideration" to conducting an external PIA before proceeding with the CDR Rules.[2] It is difficult to understand a decision to ignore a recommendation from the Australian Information Commissioner on a privacy issue. The decision to ignore that recommendation is, in our view, reckless and negligent.

Treasury engaged an external consultant, Lockstep Consulting, to review the CDR PIA and a Consulting report was released (the Lockstep Report). Lockstep Consulting did not consult any stakeholders in making the report. The Lockstep Report did find that the Treasury PIA underestimated threat likelihood in a number of key areas. The Final Treasury PIA did not address these issues in any effective way. Those risks remain ongoing and unaddressed. The CDR Rules must address those risks as much as possible.

[1] See https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments

[2] See evidence from Ms. Falk, Australian Information Commissioner, OAIC at Senate hearing on 6/3/19 transcript available at https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Fcommsen%2F0db2baf3-52a7-44b8-afa6-86bcddd194ff%2F0006;query=Id%3A%22committees%2Fcommsen%2F0db2baf3-52a7-44b8-afa6-86bcddd194ff%2F0000%22

As a PIA is an iterative process, an external PIA should be performed before proceeding with enacting the CDR Rules. Of course, it would have been far preferable to do an external PIA from the beginning of this process so that "privacy by design" principles could have been rigorously integrated into the process. That opportunity has been lost. However, the opportunity to at least rectify this flawed process should be seized now.

Recommendation 2

The CDR Rules should not proceed until an external PIA has been conducted. The recommendation by the OAIC should be adopted to do an external PIA as a matter of urgency.

Rushing through the CDR

We remain concerned about the CDR legislation rush. The rush seems to be based on an assumption that a data portability right (which is what the CDR is) will deliver significant competition benefits for people. At this stage, the evidence that this will occur is not significant or persuasive. The UK has had open banking for over a year and the uptake has been slow.

Rushing through legislation without getting the privacy safeguards in place is not in the interests of anyone.

Good for business, bad for people?

The Foundation continues to be concerned that the CDR will deliver enormous benefits for business (particularly FinTech) and not for people (and particularly be bad for vulnerable people). The CDR has been pushed heavily by business. There is no groundswell of people writing to parliament asking and begging for data portability. People already have access to their own personal information and have had that access for a significant time.

The main innovation to be delivered is that a third party will analyse that portable data and deliver a benefit to someone by finding them a "better deal". Our concern is and remains that the data is more valuable than the service being advertised. This can lead to the perverse incentives problem which is where the service provided is junk and the real effort is to get access to the data.

There is a risk with data sharing that can only be mitigated not eliminated. Data portability will leave some people very vulnerable to harm from the misuse of data including scams, poor deals, selling data, data breaches, transfer to poor value or unsuitable products, to name a few. The assumption that business will comply with the law is naïve. The revelations of the Financial Services Royal Commission demonstrated this problem. Facebook's privacy breaches are another example.

The Foundation remains concerned that the above issues are not addressed by the current drafting of the CDR Rules. In our view, the CDR Rules need to prioritise prevention and not just rely on the ACCC to enforce. We already know that people are

poorly compensated for data breaches in Australia. The loss is difficult to demonstrate. The justice system is difficult even with the free Australian Financial Complaints Authority (AFCA). This is why prevention is essential. The Foundation has drafted its submission with this emphasis.

The Foundation urges reflection, noting that the benefits to business and consumers in the United Kingdom – often considered to be the benchmark – have not been as great as forecast by enthusiasts for the CDR.

The CDR must be a closed system

The CDR Rules need to make it clear that it is a closed system. This needs to be drafted as a specific point.

Recommendation 3

The CDR must be a closed system and this must be reflected in the CDR Rules as a specific point.

Zero-tolerance approach and accredited data recipients

The CDR Rules must have a zero-tolerance approach to unauthorised disclosures by accredited persons. This is the only way to ensure that people can trust the system. It also sends a strong message to users of the system.

Any unauthorised disclosure should receive an automatic penalty as follows:

a) Immediate exclusion from the CDR
b) Automatic set compensation for the affected consumers

It is noted that this was recommended in the Lockstep Report. This should be adopted and drafted explicitly into the CDR Rules.

Recommendation 4

A zero-tolerance approach to unauthorised CDR breaches of data by an accredited data recipient.

Part B – Specific comments on the CDR Rules

Part 1 – Preliminary

1.8 Meaning of CDR Contract

1.8(3)(c) of the CDR Rules refers to an option to terminate a "CDR contract within a reasonable period, that is specified in the contract". People are unlikely to read contracts or

know what a reasonable period should be. The option to terminate should be a set period in the CDR Rules. We suggest that a reasonable period to terminate the contract is 7 days and this should be specifically set in the CDR Rules.

Recommendation 4

Section 1.8(3)(c) should specify 7 days as the reasonable period to terminate the contract.

Consumer dashboard

The dashboard should contain information about a request to delete information and the date that information was deleted.

Recommendation 5

The dashboard should contain information about deletion of data including the date of request, the data deleted and when it was deleted.

Part 2 – product data requests

No comment

Part 3 – Consumer data requests made by CDR consumers

3.5 Refusal to disclose in response to consumer data request

Many people are at risk of being a victim of scams. The ACCC has done a lot of work in trying to prevent scams. Financial institutions have a critical role in preventing scams. The refusal should contain a specific section that allows refusal where the data holders reasonably suspects the consumer is the victim of a scam. It is noted that the "risk of harm" may cover the scam, however, this section should specifically cover this risk as it is likely to happen.

Recommendation 6

Refusal on the basis of the reasonable suspicion of a scam should be a specific reason for refusal under the CDR Rules.

Fees

It is unclear why the notes regarding the fact a fee cannot be charged does not reference the source of this point.

Part 4 – Consumer data requests made by accredited persons

CDR Contracts

The Foundation remains concerned about the terms and conditions in CDR contracts. The CDR contract needs to be clearly drafted and cover:

- The consents being given
- The right to have data collected deleted
- How to access and use the dashboard
- How to withdraw consent
- The rights and details of how data held can be deleted
- How to make a complaint include details of IDR and the EDR scheme

People rarely read contracts. The information needs to be set out carefully (and tested for understanding) for disclosure to be effective. The CDR Rules have not effectively covered the form and details of the CDR contract.

The Foundation remains concerned that people will sign contracts they do not understand and pay fees for a service they do not want.

4.5 Data holder must ask CDR consumer to authorise disclosure as soon as practicable

If a consumer has asked a third party to organise access, that third party should arrange authorisation. Receiving a request for authorisation from the data holder is likely to cause confusion. This section also provides an incentive for the accredited person to move the authorisation process onto the data holder.

Recommendation 7

Section 4.5 should be deleted.

4.7 Refusal to disclose in response to consumer data request

This section should also specifically cover scams as a reason for refusal.

4.8 Use and disclosure of data collected pursuant to consumer data requests under this part

For the purposes of 4.8(3)(b) the outsourced service provider should be the agent (or legally responsible) of an accredited data recipient at law. This is to ensure that the accredited data recipient is legally responsible for the actions or failures of the outsourced service provider.

Recommendation 8

The accredited data recipient should be fully and completely responsible at law for any outsourced service provider.

4.3 – Consents to collect CDR data

The Foundation remains concerned that consent to collect data is ineffective. We appreciate that the CDR Rules are attempting to ensure that consent meets the list in 4.10(1). However, the guidance in the CDR Rules (with the best of intentions) may not actually be effective in getting informed consent.

We recommend that the following further protections are required:

- A requirement that each consent is discussed separately;
- Detailed guidance on how to comply with this section
- Draft the consents in accordance with the CDR Rules and require the use of those set consents; and
- Test the effectiveness of the consents with independent consumer testing.

Consumers must have the right to specify the time limit for the consent. The maximum time limit should be limited to 6 months and not 12 months. It is unclear why any consent would be required for 12 months.

Recommendation 9

As detailed above, further protections are required to ensure that consumers give informed consent.

4.11 Withdrawal of consent to collect CDR data and notification

Two options are provided to withdraw consent. This is not enough for people who may be vulnerable including having a disability. A range of communication methods is required to ensure accessibility.[3] This should include a range of communication methods including at least phone (with the withdrawal confirmed in writing by the accredited person), email (with a published email address) and the consumer dashboard (which also must be confirmed in writing by the accredited person). It would be preferable to also include webchat and text.

The principle must be that withdrawal of consent must be easy and accessible with a prescribed range of communication methods. For any communication method that does not give the consumer written confirmation, the accredited person must confirm that the consent has been withdrawn in writing.
The details of communication methods available to withdraw consent must be set out in any CDR contract and available on the accredited person's website.

Recommendation 10

Withdrawal of consent must be easy and accessible with a range of communication methods. This recognises the needs of vulnerable consumers to have a range of

[3] See Competitions and Market Authority UK, Consumer Vulnerability: Challenges and potential solutions February 2019, page 7 at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/782542/CMA-Vulnerable_People_Accessible.pdf

communication methods as some communication methods are simply impossible for some people.

The communication methods must include phone, email and the consumer dashboard as a minimum. The accredited person must confirm the withdrawal of consent in writing.

Part 5 Rules relating to accreditation

No comment.

Part 6 – Rules relating to dispute resolution

Internal dispute resolution

Dispute resolution is a key consumer right. We support the inclusion of a specific requirement to comply with ASIC Regulatory Guide 165.

There are a number of requirements that should also be explicitly included on internal dispute resolution that are covered in RG165 but they are drafted as recommendations not requirements. Further protections to be included:

- That the IDR contact details need to be included in the CDR contract. The IDR contact details must include a range of ways to make a complaint including phone, email and by post. (RG165.113 is more of a recommendation rather than a prescribed standard)
- The IDR process must be free (RG165 says IDR "should" be free – guiding principle 4.6.)

Recommendation 11

IDR must be free and IDR must have a published range of contact details including phone, email, and post.

External dispute resolution

Part 7 – Rules relating to privacy safeguards

7.2 Rules relating to privacy safeguard 1 – open and transparent management of CDR data

Outsourced service providers

The Foundation remains concerned about the use of outsourced service providers where personal information will be stored overseas. The risk of data misuse is heightened if the data goes overseas. Consumers should have the ability to refuse permission for data to move overseas as part of any service. This should be included in the consent process.

7.2(3) Making a complaint

There must be a range of accessible ways to lodge a complaint including a dedicated email address, phone, and mail.

7.2(3)(a) RG165 makes it clear that a complaint can be lodged with anyone at the organisation and does not need to be made to a particular department. Any attempt to limit that right would be inconsistent with RG165.

7.2.(3)(c) is not consistent with RG165. A complaint (actually an expression of dissatisfaction) can be made at any time.

7.2(3)(g) The time periods for IDR processes is set in IDR and is currently 45 days. This should not be varied.

7.2(3)(h) is unclear. A dispute resolution process should not limit options for redress as the parties should be flexible.

7.2(3)(i) should specifically require the details of the external dispute resolution scheme.

Recommendation 12

The list under making a complaint should be revised to accord with RG165.

7.4 Rules relating to Privacy safeguard 5 – notifying of the collection of CDR data

Supported.

7.5 Rules relating to privacy safeguard 6 – use or disclosure of CDR data by accredited data recipients

The Foundation does not support (and strongly objects to) any decision to allow the transfer of data between accredited persons even with consumer consent. We cannot see the benefit for the consumer. We are very concerned that further data sharing exposes the consumer to even more risk. The consumer is likely to lose track of the transfer of data and feel unempowered about the actual control of their data.

Recommendation 13

The transfer of data between accredited persons should be prohibited.

7.6 Rules relating to privacy safeguard 10 – notifying of the disclosure of CDR data

Supported.

7.7 Rules relating to privacy safeguard 11 – quality of CDR data

Supported.

7.8 Rules relating to privacy safeguard 12 – security of CDR data held by accredited data recipients

Deidentification is not an appropriate way to safeguard data. It does not work.[4] This was also acknowledged in the Lockstep Report. All deidentification is at risk of being reidentified. That risk continues to increase as our social media footprint continues to grow. It is simply not good enough to de-identify data. Data breaches also occur regularly on a "when not if" basis. Data must be destroyed when no longer being used to protect the consumer. Any other method leaves the consumer exposed to a data breach and reidentification.

If the ACCC proceeds on a reidentification basis there must be strict liability for a data breach with automatic compensation for the consumer of a significant amount. It is completely foreseeable that deidentified data can be reidentified. In those circumstances, there must be strict liability.

Recommendation 14

Data must be destroyed not reidentified.

7.9 No fee for responding to or actioning correction request

Supported.

7.10 Rules relating to privacy safeguard 13 – steps to be taken when responding to correction request

Supported.

The right to delete data

Consumers must have the right to delete data and this right needs to be covered in detail in the CDR Rules. The current draft does not cover this right. Without a right to delete the data held by an accredited person, the consumer does not have adequate control of their own data.

This is yet another example of the poor privacy laws in Australia. The right to delete should be in the Australian privacy laws. It is not. The consultation on the CDR clearly covered a right to delete. Yet now the Rules are drafted that promised right has disappeared. This is completely unacceptable.

Any promise that CDR will be empowering consumers to effectively use their own data is a lie without a right to delete. This right is the only effective consumer protection right to stop data breaches and misuse of the data. Every other security measure including deidentification, firewalls, passwords etc is poor and ineffective compared to the data being deleted.

[4] See for example, the reidentification of Medicare data reported in 2017 at https://www.abc.net.au/news/science/2017-12-18/anonymous-medicare-data-can-identify-patients-researchers-say/9267684.

Recommendation 15

There must be a comprehensive right to demand the deletion of data in the CDR Rules.

Civil penalties

We look forward to being consulted on this essential section.

Schedule 2 Part 3 - Joint accounts

The Foundation remains concerned that the CDR Rules on joint accounts are inadequate to protect vulnerable consumers.

Family violence

There needs to be a mechanism in place to suppress personal information for anyone who fears for their safety. This might be a sole account or joint account. Consumer advocates are asking banks to develop "silent accounts" and flags to protect information for people who may be unsafe. The CDR Rules need to explicitly give the bank to reuse access to any flagged or silent account with safety concerns.

There is no doubt that account information can be used to find people and accordingly put a person at risk of serious harm or death.

There also needs to be a mechanism in place for the data holder to ensure that information is not inadvertently provided in these circumstances on request.

Joint accounts

The joint account management service as set out in the CDR Rules is unlikely to provide any protection for anyone under duress. This proposed solution needs a lot more consultation.

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
[redacted]