



**Australian
Privacy
Foundation**

<http://www.privacy.org.au>

Secretary@privacy.org.au

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

21 October 2019

Maddocks

By email:

RE: Draft Privacy Impact Assessment – Consumer Data Right

This submission from the Australian Privacy Foundation (The “APF”) responds to the draft Privacy Impact Assessment (PIA).

General comments

The APF has been given very little time to respond to a very lengthy PIA. Accordingly, this has limited our ability to consider the PIA in depth and respond in detail. The APF spent considerable time campaigning for an independent PIA and we are disappointed that we get very little time to consider it and respond.

The fairness and engagement in this PIA process has been poor from the start. The PIA was an afterthought by Treasury. It then delivered a draft PIA conducted by itself (which was not independent). This is despite already enormous problems that arose from “in house” PIAs used for the 2016 census and My Health Record. The consultation occurred over Christmas and then the PIA was finalised soon after with the addition of an extra report. Finally, after near universal condemnation of the failure to do an independent PIA (including from the OAIC), Maddocks was commissioned to do the PIA. In the meantime, the relevant consumer data right legislation has been enacted.

A good PIA process (as confirmed by the OAIC) embeds privacy issues from the start. Although privacy was mentioned from the start in the ACCC process, it was not embedded into the design in any meaningful way. This deprived everyone of the benefit of a consumer data right that had privacy as a key design focus. An example of how privacy was forgotten was that the consumer data right legislation introduced into parliament did not have a right to delete. That right now only appears in the Draft Rules and subject to a right of de-identification to be elected by the data holder. We would argue that a genuine privacy by design process would have delivered a right to delete enshrined into the legislation.

The ACCC has since made numerous recommendations to strengthen privacy laws in Australia following the Digital Platforms Inquiry. These reforms are strongly supported by the APF. These reforms are not just necessary for privacy protections when using digital platforms, they are also

necessary protections when using the consumer data right. The Government has not committed to make the legislative changes recommended by the ACCC to date. We believe that these recommendations must be implemented urgently so people are adequately protected if they use the consumer data right.

The recommendations in the PIA

Recommendation 1

The APF supports recommendation 1 in the PIA. The PIA must be a living document. There must also be a list of criteria that will trigger a review of the PIA. We support the criteria currently listed.

We do not agree that it is sufficient for there to be a public commitment to the criteria set. We believe there is a high likelihood of those requirements being overlooked or forgotten. The criteria must be added to the CDR Rules. This would ensure that any changes would trigger action from a regulator to instigate a review of the PIA.

Recommendation 2

We support recommendation 2. In general, guidance is only useful for industry. However, as it is important that industry comply with all standards, detailed guidance may assist. We remain very sceptical about how effective any guidance will be but it is better to have it rather than not.

We confirm that the APF is a stakeholder that consistently confirms that consumer education as a response to addressing the compromises and threats to their interests embedded in the flawed CDR model, and the likely systemic abuse of a consent model that cannot properly reveal or protect their interests. Just as the systemic market failures repeatedly revealed in the Australian consumer credit and consumer finance area are now acknowledged to require more aggressive intervention on the side of the greatly weaker, in some cases almost defenceless party, the impending market and regulatory failure in the misleadingly named CDR model also require moving beyond 'education' and 'consent' models which appear likely to be inadequate for the task of protecting the greatly weaker party from the depredations of a predatory global personal information exploitation sector.

Recommendation 3

The APF supports recommendation 3 subject to our comments and additions below.

Recommendation 3.1 is supported. Testing or auditing compliance is an excellent method to check whether the process is working. We would add that a process should also be included in the CDR Rules which sets out when, how and how often testing will occur.

Recommendation 3.2 is missing.

Recommendation 3.3 is supported. CDR consumers do need to be warned at relevant points in time about a possible loss in protections. As stated in many previous submissions, it is essential to deliver information to consumers when it is needed and to independently test whether that communication is likely to be effective. That said, disclosure alone is never sufficient for

consumer protection so consideration needs to be given to more effective interventions to guide consumers away from sharing information with third parties outside the CDR regime.

Recommendation 3.4 does not go far enough. Providing advice about what to do if the consents do not match is not sufficient to fix this problem. Consent is the cornerstone of making sure people have control of their personal information. Unfortunately to date, many consumers have lost control of their personal information when forced into bundled consent. We remain concerned that the consent process will remain ineffective and we will discuss that further below. If the consent does not match it must be void. The process effectively needs to start again to ensure that the consent being given is followed exactly.

Recommendation 3.5 is supported.

Recommendation 3.6 is supported with the extra requirement that not only is the conflicting contractual clause void but it can also be compulsorily removed by the ACCC. This is consistent with the ACCC's recent recommendations in unfair terms for customer loyalty schemes and digital platforms.

Recommendation 3.7 is supported. All relevant parties must be informed about the withdrawal of consent.

Recommendation 4

Recommendation 4 is supported. All the privacy principles must be reflected in the CDR. CDR consumers must be able to access their own personal information from any participant in the system which holds that information. That access should be provided free of charge.

Recommendation 5

Recommendation 5 is supported. The CDR is a complicated and confusing system. It puts consumers at a serious disadvantage when interacting with the system. At a minimum, everyone needs to know what standards are legally binding.

Recommendation 6

We do not support recommendation 6 as it is currently drafted. It is effectively a dodge around the issue and a very disappointing dodge. There are two issues:

1. The privacy of the joint account holder who has not consented to CDR; and
2. The possible consequences of that access which includes family violence (but is not limited to this issue).

To ensure privacy rights are safeguarded, joint account data should not be portable unless consent is obtained from both account holders. This is a fundamental principle for joint accounts, that is that both account holders own that personal information. It does not follow that separate access to money (which is set up by consent) means that the personal information principles have changed. Our view is that the disclosure of personal information without consent could be challenged at law. Even if that challenge is not successful, the provision of that data to a third party without consent remains a serious breach of privacy.

It is unclear how a PIA can be meaningfully done without a serious and lengthy consideration of this issue. Instead, this PIA has flagged a possible problem but avoided serious analysis. There is no doubt at all that allowing personal information to be provided to third parties without consent will endanger some people. It is also likely to be misused to facilitate switching accounts without consent.

There is a serious privacy impact on joint account holders. We recommend that the personal information in a joint account cannot be shared without joint consent. If this recommendation is not adopted there must be minimum protections including:

1. Warnings when information is shared;
2. Improved consents for new accounts that flag this possibility and provide options on how it will be managed; and
3. Providing consumers the options to change consents with the bank to prevent sharing without joint consent.

Recommendation 7

This recommendation is not supported. It is unclear why third party data can be shared with anyone else without their specific consent. When that data was provided by the third party it was for a specific purpose. It is now being handed over to another third party. This could never have been anticipated. It is likely that some third party data (such as payments) will be incredibly valuable in the wrong hands. The consumer will not go through their statements carefully and may miss the opportunity to not disclose sensitive information.

Third party information must be redacted. It cannot be shared with a third party without consent. Again, this decision is not consistent with the Australian Privacy Principles. The PIA should be amended to clearly identify this issue and recommend redaction.

Recommendation 8

Recommendation 8 is supported.

Recommendation 9

Recommendation 9 is supported. The APF is continually disappointed with the funding and the regulatory approach of the OAIC. The OAIC is a very weak and powerless regulator. Unfortunately a lot of it's work (including litigation) is performed by the ACCC. Weak regulators are a poor outcome for everyone.

Recommendation 10

Recommendation 10 is supported.

The privacy issues that have not been covered

The right to delete

De-identification does not work. De-identified data is relatively easy to reidentify. This ease continues to increase over time. When a data holder de-identifies data they are effectively making it so they continue to have access to the data. It is basically a cheat. It is a way to keep the data and to fool the consumer into believing it is safe, when it is not.

People must have a right to delete any data that is provided. The current CDR Rules do not appropriately deal with this issue. The PIA has not identified the serious risks with de-identification or the risks for the consumer. There is not even a provision to warn the consumer that de-identified data is not safe or secure.

Control of personal information means that when the consumer no longer wants the data holder to have the information it must be deleted. We agree that the only exceptions should be in the event of a live dispute or where deletion would be against another law.

A closed system

It must not be possible to receive or deal with data unless that party is registered in the CDR regime. The CDR regime is so complex we remain unsure as to whether this requirement has been met. We do not believe it has. The CDR Rules need to make it that it is unlawful to disclose any data to a recipient that is not a member of an EDR scheme (apart from the consumer). There must not be any exceptions for any purpose. The consumer must at all times have control of their personal information and be able to make a complaint about any part of the process to an EDR scheme.

Conclusion

We refer to the APFs previous submissions on the PIA. In many respects the same concerns remain: the belatedly and reluctantly tacked-on second PIA has not been able to address the flawed model and threats to consumer interests embedded in the CDR scheme, or the unsustainable assumptions about de-identification and other ostensible controls on data abuses and inevitable breaches and abuses of personal data and data protection. It still seems more likely to be a de facto fintech and data hackers' right than a consumer right, especially in the ongoing absence of a right to sue for breach of privacy or data protection in this country (almost alone among comparable countries despite three decades of recommendations that this central 'consumer data right' is needed here).

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

Yours sincerely

A handwritten signature in blue ink, appearing to read 'Kat Lane', with a stylized, cursive script.

Kat Lane,
Vice-Chair
0447 620 694
Kat.Lane@privacy.org.au