Australian Government

Office of the Australian Information Commissioner

Inquiry into Future Directions for the Consumer Data Right – Issues Paper

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

21 May 2020

OAIC

Contents

Overview

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Issues Paper for the Inquiry into Future Directions for the Consumer Data Right (CDR). The Issues Paper outlines how the functionality of the CDR system could be expanded to increase innovation and competition in future and how it could leverage relevant international developments. In particular, the paper considers how the CDR system could be expanded to include 'write' access.

By way of overall comment, the OAIC is broadly supportive of proposals to expand the CDR system to increase innovation and competition, provided this expansion is underpinned by strong privacy protections. In this regard, the OAIC supports the central focus of the Inquiry on privacy and security, as well as on ensuring that any expansion of the CDR system protects vulnerable consumers.

Expanding the CDR system will lead to increased data flows across and within sectors, with further potential for sensitive data sets to be combined and to provide richer insights about individuals. Any expansion to the scope of the CDR to allow write access, would therefore require careful consideration of the associated security risks. Accordingly, in order to ensure consumer trust and confidence in the CDR system is maintained, any expansion should be accompanied by the right privacy mitigation strategies and governance practices.

Given these factors, the OAIC considers Treasury will need to undertake a Privacy Impact Assessment (PIA) for any significant expansion of the CDR system resulting from this Inquiry, particularly in relation to write access. A PIA is a systematic assessment of a project to identify the impact it might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact.

Further, the *Privacy (Australian Government Agencies – Governance) APP Code 2017* requires agencies subject to the *Privacy Act 1988* (Cth) (Privacy Act) to conduct a PIA for all 'high privacy risk' initiatives that involve new or changed ways of handling personal information.[1] The PIA on the CDR system undertaken by Treasury (as well as the subsequent independent iteration of the PIA undertaken by an external law firm) also acknowledged that further PIAs may be necessary as various components of the CDR are revised or extended.[2]

Recommendations

1. In order to consider the privacy impacts of any expansion of the CDR to include write access, we recommend that Treasury undertake a PIA before implementing any significant expansion to the CDR scheme as a result of this Inquiry. The PIA process should be undertaken early to allow the findings to influence the development of the write access model and any supporting rules.

[1] Section 12 of the *Privacy (Australian Government Agencies – Governance) APP Code 2017* provides that a project may be a high privacy risk project if the agency reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

[2] The Treasury, Consumer Data Right: Privacy Impact Assessment, 1 March 2019 and Maddocks, Consumer Data Right Privacy Impact Assessment, December 2019.

2. In addition to conducting a PIA as per Recommendation 1, the OAIC recommends any tiered accreditation models developed to allow broader participation within the CDR system should maintain appropriate privacy settings, to ensure high levels of consumer trust in the system.

3. The OAIC recommends implementing privacy risk mitigation strategies in relation to any direct consumer access to CDR data.

4. All entities that handle CDR data, including accredited data recipients at all tier levels, data holders, designated gateways, outsourced service providers and any other entities which may participate in the CDR system in future, should be bound by the Privacy Act in their handling of any personal information that is not CDR data.

5. The OAIC supports the Inquiry's focus on leveraging developments from international jurisdictions, and recommends a focus on strengthening interoperability to ensure that CDR data is protected regardless of where it flows.

About the OAIC and our role in the CDR system

The OAIC is Australia's independent regulator for privacy and freedom of information. The OAIC co-regulates the CDR scheme together with the Australian Competition and Consumer Commission (ACCC). The OAIC enforces the privacy safeguards (and related CDR Rules) and advises the ACCC and Data Standards Body on the privacy implications of the CDR Rules and Standards. The OAIC is also responsible for undertaking strategic enforcement in relation to the protection of privacy and confidentiality, as well as investigating individual and small business consumer complaints regarding the handling of their CDR data.

Our goal in regulating the privacy aspects of the CDR system is to ensure that the system has a robust data protection and privacy framework, and effective accountability mechanisms to ensure consumers are protected.

Potential expansions to write access

The Issues Paper examines how the CDR system could be expanded to include 'write access', which describes any process where a trusted third party could change or add to data about a consumer (with their consent).[3] The OAIC understands write access could also allow consumers to authorise trusted third parties to make payments on a consumer's behalf, and apply for, manage and change products for consumers through application programming interfaces (APIs).

The OAIC is broadly supportive of expanding the operation of the CDR to include write access, recognising the cross-sector benefits it may have in improving innovation and increasing competition.

Further, the expansion to write access would provide a safer alternative to screen scraping, a practice which carries considerable privacy risks. Allowing write access would reduce the prevalence of screen scraping, as trusted third parties will be able to modify consumer data with their consent, within the protections of the CDR ecosystem. The expansion of the CDR system to include write access may therefore present an opportunity to restrict other less secure methods of providing access to financial data (such as screen scraping).

However, the expansion to write access may also raise new privacy and security implications, which will need to be appropriately addressed. In particular, as write access would allow third parties to modify a consumer's financial information, it may increase the motivation for unauthorised actors to target an accredited data recipient's information system. Mitigations would also need to be considered to ensure new security concerns do not emerge, such as phishing schemes.

Unauthorised access to (or disclosure of) sensitive financial data can have significant consequences for individuals, particularly vulnerable consumers. For example, the mishandling or misuse of consumer data could lead to financial fraud, identity theft, and associated economic and psychological harm and distress for affected individuals.[4]

Strong privacy mitigation strategies will therefore be required to reduce any risks associated with an expansion to write access. To ensure these risks are appropriately identified and addressed, the OAIC

[3] Issues Paper, p.5.

[4] See, eg, the discussion in the Explanatory Memorandum to the *Privacy Amendment (Notifiable Data Breaches) Bill 2016*.

recommends that Treasury undertake a PIA before expanding the CDR system to a write access model.

Recommendation 1

In order to consider the privacy impacts of any expansion of the CDR to include write access, we recommend that Treasury undertake a PIA before implementing any significant expansion to the CDR scheme as a result of this Inquiry. The PIA process should be undertaken early to allow the findings to influence the development of the write access model and any supporting rules.

Potential expansions to read access

The Issues Paper considers a range of potential options that could expand the current scope of 'read access' functionality, which describes any process where a consumer can transfer CDR data to a trusted third party, which can be read but not modified.[5]

The OAIC understands that the Inquiry will consider a range of issues, including a standard 'consent taxonomy', expanding the types of CDR participants and service providers in the CDR system, and how a tiered accreditation model may support this. In view of the broad range of matters raised regarding read access, the OAIC's comments are focussed on the privacy impacts associated with enabling greater participation and tiered accreditation, as these would likely have a significant impact on the existing privacy framework within the CDR system.

Expanding participation to non-accredited third parties

The OAIC recognises that expanding the types of actors that can participate in the CDR system may enable greater participation from interested parties, potentially promoting innovation and allowing new products and services to be offered to consumers. However, any such expansion of the CDR system should also maintain the strong privacy protections and safeguards that currently exist within the system.

The existing protections reflect the sensitive nature of CDR data and are designed to prevent misuse of the data and build consumer trust in the system. For example, a central privacy protection of the system is the accreditation framework, which promotes trust by requiring entities to satisfy a range of accreditation criteria, prior to the transfer of any consumer data.

The OAIC would therefore caution against an expansion of the CDR system to allow non-accredited third parties to participate, unless there are compelling policy reasons to allow data transfers to such parties, and adequate mitigation strategies can be put in place to address the associated privacy risks.

[5] Issues Paper, p.5.

Tiered accreditation

To reduce the risks associated with wider participation in the CDR framework, the Issues Paper considers introducing tiered levels of accreditation.[6] The OAIC understands that tiered accreditation would reduce barriers to entry, as some entities may find the full accreditation requirements financially and technologically burdensome. Under a tiered accreditation system, entities could instead comply with a lower level of accreditation requirements, accompanied by risk-based restrictions on access and use.

The OAIC recommends that any changes to accreditation requirements should be carefully tailored to mitigate the risks posed by the specific data handling activities of the relevant entities, and in a way that ensures the privacy and security risks are managed consistently across the scheme and that the overall integrity of the CDR system is maintained.

Recommendation 2

In addition to conducting a PIA as per Recommendation 1, the OAIC recommends any tiered accreditation models developed to allow broader participation within the CDR system should maintain appropriate privacy settings, to ensure high levels of consumer trust in the system.

Consumers directly accessing their own CDR data

The Issues Paper notes that as the CDR system evolves, consumers will be provided with greater opportunities to have control over and access to their own data.[7] In principle the OAIC supports consumers having the ability to directly access their own data. Providing consumers with increased access to their own data is consistent with fundamental privacy principles.

However, the OAIC is aware that there may be risks associated with providing access directly to consumers. Given the sensitivity of CDR data, this may increase the security and privacy risks for a consumer, if they were to provide such data to an unaccredited third party, outside the protection of the CDR framework. The risks are likely greater for vulnerable consumers, who may be incentivised or pressured by malicious actors into disclosing their sensitive CDR data. In addition, in the absence of restrictions entities may request access to an individual's CDR data, effectively making this a pre-requisite for the provision of goods or services.

While the CDR Rules currently provide that a consumer can make a request for access to their own CDR data, the relevant standards have not been developed to enable this.[8] The OAIC supports this approach for the early implementation phase. However, we recommend that careful consideration should be given to how direct access could be facilitated in future, and in particular what privacy risk mitigation strategies need to be put in place to protect consumers and retain consumer trust.

[6] Issues Paper, p.5.

[7] Issues Paper, p.7.

[8] CDR Rule 3.3 allows a consumer to make a request for their data, but standards to implement this have not been developed.

One potential mitigation strategy may be to introduce restrictions on certain types of non-CDR entities asking consumers to provide their CDR data. This would build on a similar approach under Part IIIA of the Privacy Act, which prohibits all entities except credit providers from requesting direct access to an individual's credit report from a credit reporting body (excluding all others from access, importantly real estate agents, landlords, employers, and insurance companies).[9]

Recommendation 3

The OAIC recommends implementing privacy risk mitigation strategies in relation to direct consumer access to CDR data.

Privacy Act coverage for all CDR entities

Given the sensitivity of CDR data, and the potential for any expansions to the CDR system to result in more complex data flows between and within entities, it is critical that there are privacy protection and governance mechanisms in place for all of the personal information which may be handled by CDR entities.

The OAIC considers that all entities participating in the CDR system should be bound by the Privacy Act in relation to all personal information held by the entity, including personal information that is not CDR data. While the CDR system has extended the protection of the Privacy Act in this way to accredited persons (via s 6E(1D) of the Privacy Act), there is no equivalent provision for other entities that handle CDR data. While many of these entities (such as data holders) are likely to be subject to the Privacy Act already, some entities may not be where they are small businesses.[10]

The OAIC therefore recommends that s 6E(1D) of the Privacy Act be expanded so that all data holders, designated gateways, outsourced service providers and any other entities which may participate in the CDR system in future are bound by the Privacy Act in relation to any personal information that is not CDR data. Extending coverage in this way will ensure that there is a baseline level of protection for the handling of personal information in all CDR entities. Further, the OAIC recommends that accredited persons at all future potential tier levels should be subject to the Privacy Act, which will help to retain consumer trust in the CDR system.

Recommendation 4

All entities that handle CDR data, including accredited data recipients at all tier levels, data holders, designated gateways, outsourced service providers and any other entities which may participate in the CDR system in future, should be bound by the Privacy Act in their handling of any personal information that is not CDR data.

[9] See, eg, s 6G(5) of the Privacy Act and s 10 of the *Privacy Regulation 2013*.

[10] See s 6C of the Privacy Act.

Leveraging international developments

The Issues Paper notes that the Inquiry presents the opportunity to increase interoperability between Australian and international jurisdictions, in relation to data portability and open banking frameworks. Interoperability does not mean uniformity – but rather recognises the differences in regulatory frameworks and provides a bridge to ensure that information is protected, regardless of where it flows.

In particular, the Issues Paper notes the recent developments in several international data portability and open banking regimes, including the United Kingdom's Open Banking regime and the European Union's Payment Services Directive 2, but also emerging regimes in Singapore, Hong Kong and Canada.[11]

Given the global nature of data flows, the OAIC is actively engaged in a range of international privacy and data protection forums, ensuring shared expertise and cooperation on cross-border privacy matters, including through the Global Privacy Assembly.[12] One of the key objectives in forging these and other international partnerships is to enhance the interoperability of Australia's privacy regime with the various data protection frameworks around the world. The OAIC is therefore supportive of the Inquiry's focus on leveraging developments and experiences from other jurisdictions, and would welcome the opportunity to be consulted further and assist on these issues as policy developments progress.

In the OAIC's view, one key area for further assessment and consideration would be the United Kingdom and European Union's prohibition of unsafe online practices (such as screen scraping by non-accredited third parties), and how this could be leveraged to assist with future developments in the CDR.

Recommendation 5

The OAIC supports the Inquiry's focus on leveraging developments from international jurisdictions, and recommends a focus on strengthening interoperability to ensure that CDR data is protected regardless of where it flows.

[11] Issues Paper, p.4.

[12] Formerly, the International Conference of Data Protection and Privacy Commissioners.