Australian Government

Office of the Australian Information Commissioner

Select Committee on Financial Technology and Regulatory Technology – Issues Paper

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

10 December 2020

OAIC

December 2020

Contents

Overview

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the second Issues Paper published by the Senate Select Committee on Financial Technology and Regulatory Technology (the Committee).

The second Issues Paper (Issues Paper) is seeking views on a broad range of longer-term reforms that are aimed at supporting the development of technology to drive economic growth in Australia, for example in relation to tax, regulation, capital, culture and skills. This includes a consideration of the Consumer Data Right (CDR), and whether additional requirements should be placed on certain types of accredited data recipients (such as large non-bank technology companies) to ensure a level playing field. The Committee is also seeking views on the rollout of the CDR to additional sectors (including other sectors in the financial services industry), and how best to leverage the long-term potential of the CDR.

By way of overall comment, the OAIC acknowledges the important policy objectives of the Issues Paper, which include maximising opportunities for technology in Australia, including through the CDR system. The CDR system aims to encourage innovation and competition between service providers, helping consumers to access products and services that better suit their specific needs. However, if the full potential of CDR technology and innovation is to be realised in a sustainable way, privacy must remain integral to the equation. While the CDR is still in its early stages of operation, indications are that successful data driven reforms need to have a strong privacy foundation, with consumers now ranking data privacy as the top consideration when choosing a digital service.[1]

There are a number of features that ensure a strong privacy foundation for the CDR, such as having safeguards and mechanisms in place to ensure that accredited data recipients handle CDR data appropriately.[2] However, another key factor is having relevant privacy obligations oversighted by the OAIC, the national independent privacy regulator. These measures help to engender public trust, and build a social licence for organisations to engage in new data-related activities. They also help to ensure that if CDR data is mishandled, individuals have access to appropriate accountability mechanisms, and good data-handling practices are embedded by industry.

In order to assist the work of the Committee, this submission outlines the responsibilities of the OAIC under the CDR system, the co-regulatory approach to maintaining the integrity of the CDR, and the privacy protections that underpin the system.

This submission also makes three key recommendations.

First, the OAIC recommends that the Committee consider both the existing CDR privacy regime and the broader domestic privacy landscape (including the *Review of the Privacy Act 1988*), as important context for any long-term regulatory reform regarding technology.

Second, we recommend that the strong privacy protections in the system are preserved, including by continuing to have the OAIC, as Australia's national independent privacy regulator, oversighting the privacy aspects of the CDR.

Finally, in light of large non-bank technology companies potentially participating in the CDR, we recommend that the Committee consider whether there are specific uses or disclosures of data that

[1] In the OAIC's Australian Community Attitudes to Privacy Survey 2020 (2020 ACAPCS), it was revealed that data privacy is now the top consideration when choosing a digital service — ahead of all other considerations such as quality, convenience or price. More than half of Australians (55%) rank 'my data privacy' as the most or second most important element at the time of choosing a digital service, making privacy far more important to Australians than the reliability of the service or app (35% rank this first or second).

[2] These privacy-enhancing features are outlined further in the submission below.

should be prohibited in the CDR (rather than relying on an individual's ability to consent to protect them). For example, the Committee could consider recommending the prohibition of certain information handling practices through further 'no-go zones'.[3]

Broader policy context for privacy and technology related reforms

The OAIC notes there are a number of policy developments underway which may facilitate the expansion of the CDR that the Committee may wish to consider when making any recommendations, including the Inquiry into Future Directions of the CDR, and the Australian Competition and Consumer Commission's (ACCC) recent consultation regarding the proposed CDR rules expansion.[4]

There are also a broad range of other policy initiatives underway that seek to address issues in the broader privacy landscape, as well the privacy-related and other ethical impacts of the activities of large technology companies. For example, the ACCC's Digital Platform Inquiry helped to unveil the extent of data used by these entities, as well as the information asymmetry between digital platforms and the individuals whose data they utilise. A key reason given by the Australian Government for initiating this review was the increasing importance of responding to privacy risks to ensure consumers and businesses have trust, confidence and capacity to engage in the digital world.[5]

The Government's Response to the Digital Platform Inquiry committed to a broad review of the *Privacy Act 1988* to ensure it empowers consumers, protects their data and best serves the Australian economy. The review commenced in October 2020 and is being led by the Attorney-General's Department.[6] The review provides an opportunity to consider the broader privacy regulatory infrastructure that supports the Australian economy. Terms of reference for the review include:

- the scope and application of the *Privacy Act 1988* (Privacy Act)
- whether the Privacy Act effectively protects personal information and provides a practical and proportionate framework for promoting good privacy practices
- the effectiveness of enforcement powers and mechanisms under the Privacy Act and how they interact with other Commonwealth regulatory frameworks.

The Government's Response to the Digital Platforms Inquiry also confirmed the Government's commitment, first announced in March 2019, to develop legislation to amend the Privacy Act to increase maximum civil penalties to match penalties under the Australian Consumer Law, and to require the development of a binding privacy code that will apply to social media platforms and other online platforms that trade in personal information. Consultation on this draft legislation is expected to commence in the coming months.

The OAIC encourages the Committee to consider these privacy reforms as part of its consideration of any long-term regulatory reform regarding financial and regulatory technology. The OAIC's submissions in response to these Inquiries are available at www.oaic.gov.au/engage-with-us/submissions.

---

[3] See for example the no-go zones in the Canadian framework, which are implemented through guidance in Office of the Privacy Commissioner of Canada (2018*) Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)*, Office of the Privacy Commissioner of Canada website.

[4] ACCC, *CDR rules expansion amendments consultation paper*, 30 September 2020.

[5] The Treasury, *Regulating in the digital age - Government Response and Implementation Roadmap for the Digital Platforms Inquiry*, December 2019.

[6] Attorney-General's Department, *Review of the Privacy Act 1988*, October 2020.

Consumer Data Right

Privacy protections promote trust and confidence

The Review into Open Banking Report recognised that a high level of privacy and security protection must be a core feature for the CDR to build community trust, and ultimately to succeed.[7] The CDR has therefore been designed with both competition/consumer and privacy objectives in order to maintain the consumer confidence necessary to support innovation and economic growth. It does this by incorporating a number of world leading protections, which provide individuals with increased choice and control, underpinned by robust accountability and transparency provisions for their handling of CDR data. For example:

- **Enhanced choice and control for consumers**: Consumers must actively select which data they consent to being collected, and what specific uses they consent to. Consent is also time limited (to 12 months), and it cannot be gained as a result of default settings or pre-selected options.
- **Right to delete**: consumers can elect for their CDR data to be deleted once it is no longer needed.
- **Transparency measures**: To promote trust and confidence in the CDR scheme, accredited data recipients and data holders are required to provide consumers with an online 'dashboard' that allows them to easily track and manage their data sharing activity.
- **Prohibitions against certain activities**: including general prohibitions against selling CDR data, or aggregating CDR data for the purposes of identifying, compiling insights into, or building a profile in relation to a person who is not the consumer.
- **Enhanced penalties**: The OAIC regulates the privacy aspects of the CDR scheme and can use a range of investigative and enforcement powers under both the *Competition and Consumer Act 2010* (Competition and Consumer Act) and the Privacy Act. The penalties available for breaching the CDR system are stronger than under the Privacy Act (for example, the maximum penalty amount that can be applied under the CDR is approximately $10 million, while the maximum amount of under the Privacy Act is approximately $2.1 million).[8]
- **Accreditation framework**: participants must be accredited to receive CDR data, which provides consumers with evidence-based information about the credentials of entities with which they may engage.

The privacy protections in the CDR therefore build on the existing Privacy Act framework, but provide more specificity and an enhanced compliance framework, in light of the special need for trust in a new data portability system (and reflects that the data to be transferred is considered sensitive by the community). This strengthening of privacy protections is a recent trend occurring not only in the CDR system, but also more broadly across the domestic privacy landscape. In addition to the Digital Platform Inquiry and review of the Privacy Act mentioned above, another example is the amendments to the *My Health Records* system, which now contains specific enhanced privacy requirements, such as the right to

[7] Review into Open Banking in Australia – Final Report, December 2017.

[8] See s 56EV of the Competition and Consumer Act for the maximum amount of civil penalty provisions under the CDR system.

permanently delete a My Health Record[9] and prohibitions on certain information handling activities.[10] The OAIC is the independent regulator for the privacy aspects of the system.

The OAIC therefore recommends that the Committee considers both the existing CDR privacy regime and the broader domestic privacy landscape (including the review of the Privacy Act), as important context for any long-term regulatory reform regarding technology. Consistent with these recent policy developments and Inquiries, privacy and security should remain critical to the regulatory infrastructure that supports the CDR. In particular, the existing strong privacy protections in CDR system, including OAIC's independent regulatory role of those privacy protections, should be preserved to ensure individuals have trust and confidence in the CDR system.

OAIC's role and co-regulatory model

The CDR is co-regulated by the ACCC and the OAIC. The OAIC regulates the privacy aspects of the CDR scheme, and can use a range of investigative and enforcement mechanisms under the Competition and Consumer Act and the Privacy Act. The ACCC is responsible for the accreditation process, including accrediting potential data recipients and establishing and maintaining a Register of Accredited Persons. The ACCC has a range of enforcement powers it can use to monitor and ensure compliance with the CDR Rules. Currently the ACCC is also responsible for making the *Competition and Consumer (Consumer Data Right) Rules 2020* (the CDR Rules).

The OAIC notes that the Australian Government has recently introduced the *Treasury Laws Amendment (2020 Measures No. 6) Bill 2020*, which proposes to amend the Competition and Consumer Act by reallocating responsibility for CDR sector designation and CDR rule-making from the ACCC to the Minister. The decision on whether to reallocate these functions will ultimately be a matter for the Australian Parliament. However, the OAIC notes that while rule-making and other responsibilities may be transferred from the ACCC to the Minister, the key aspects of the co-regulatory model for the CDR system would not be affected by the proposed legislation.

The OAIC is strongly supportive of the existing co-regulatory model, as it provides the ability to focus on both the competition/consumer protection, and privacy aspects of the scheme. In particular, as outlined above, we strongly emphasise the value in having Australia's national independent privacy regulator oversighting the privacy aspects of the CDR system, as this helps to ensure consumer trust and confidence, and consistency of regulatory approach to privacy matters across the Australian economy. The OAIC also considers the co-regulatory model allows for clear and streamlined processes around policy interpretation, advice on obligations and advice and enforcement of consumer rights in the existing division of responsibilities between the OAIC and the ACCC.

Regulatory obligations on large non-bank technology companies participating in the CDR

The Committee's Issues Paper seeks views on what regulatory obligations may be appropriate for certain accredited data recipients, in light of the possibility that large non-bank technology companies may seek accreditation. The OAIC is supportive of the Committee's focus on this area, given the CDR is currently open to large non-bank technology companies, such as Google or Facebook, to become accredited under the CDR system.

Consistent with the views expressed by other stakeholders, we note the participation of these entities in the CDR may raise a range of significant privacy risks, given the volume of data already held by these

[9] See s 17(3) of the *My Health Records Act 2012*, which requires the destruction of records containing health information in a My Health Record upon request by the individual.

[10] See s 70A of the *My Health Records Act 2012* which defines prohibited purposes for the use of My Health Records which includes underwriting a contract of insurance for a healthcare recipient, determining whether a contract of insurance covers a healthcare recipient and determining the employment of a healthcare recipient.

entities. For example, it would be open to accredited data recipients to ask consumers to consent to combining sensitive financial data with the extensive amount of personal information already collected by these large technology companies (through social media profiles, messages, emails, search histories, and other sources), to deliver products or services. This would allow a large non-bank technology company accredited under the CDR to build profiles of individual consumers, and to derive and provide deep and rich insights into those individuals.

While CDR consumers must consent to such uses of data, depending on the circumstances issues may arise about a consumer's capacity to provide fully informed and voluntary consent to certain data handling practices by large non-bank technology companies.[11] These challenges and the potential for harmful impacts can be amplified for vulnerable consumers.

In the OAIC's view, there are some types of information handling practices (many of which are used by large non-bank technology companies in their existing business models) which do not meet the expectations of the Australian community. For example:

- undertaking inappropriate surveillance or monitoring of an individual through audio or video functionality of the individual's mobile phone or other personal devices. The majority of Australians (83%) feel their personal devices listening to their conversations and sharing data with other organisations without their knowledge would be a misuse of personal information.[12]
- The scraping of personal information from online platforms. The community considers the social media industry the most untrustworthy in how they protect or use their personal information (70% consider this industry untrustworthy).[13]
- The collection, use and disclosure of location information about individuals can be used to profile individuals and is difficult to make anonymous. Around 72% of older Australians were uncomfortable with digital platforms/online businesses tracking their location through their mobile or web browser.[14]
- Certain uses of AI technology to make decisions about individuals.

There are already a number of protections under the CDR system that underpin the consent-based nature of the scheme. For example the Data Minimisation Principle limits the scope of data that could be collected and used, with these entities only able to collect and use data that is 'reasonably needed' to provide a good or service requested by the consumer. There are also prohibitions in CDR against direct marketing activities (except in a narrow set of circumstances), and aggregating data for the purposes of identifying, compiling insights into, or building a profile in relation to a person *other than* the consumer themselves. These protections will place some limits on the ability of large technology companies to undertake activities that may be privacy-invasive, or involve the inappropriate or unexpected use or disclosure of data.

However, in the OAIC's view consideration could be given to whether further strengthening of the consumer protections under the CDR is required to prohibit certain uses of data under the CDR, where these uses do not meet the expectations of the Australian community. The OAIC notes that there are many other complex regulatory matters to consider in relation to such a proposal, which go beyond privacy.

---

[11] For example, the ACCC's Digital Platform Inquiry found that existing business models of global social media platforms and other digital platforms offer take-it-or-leave-it terms and conditions, which limit the ability of consumers to provide well informed and freely given consent.

[12] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 36.

[13] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 55.

[14] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 79.

The OAIC therefore recommends that the Committee consider whether there are specific uses or disclosures of data that should be prohibited in the CDR (rather than relying on an individual's ability to consent to protect them). For example, the Committee could consider recommending the creation of further 'no-go zones'. Prohibitions on information handling activities are already a feature of the CDR (for example, selling CDR data, or aggregating CDR data for the purposes of identifying, compiling insights into, or building a profile in relation to a person who is not the consumer), however, there may be other types of unethical, unfair or uncompetitive acts or practices that should be considered for prohibition.

Rollout of the CDR to financial services sectors

The Issues Paper notes the recommendation by the Committee to rollout the CDR into additional sectors within financial services, including the superannuation and general insurance sectors, in its interim report. From a privacy and information access perspective, the OAIC is broadly supportive of rollout of the CDR to these sectors and considers this has the potential to provide consumers with greater access, choice and control over their data in these sectors.

However, the OAIC notes that data flows in the superannuation sector and general insurance sectors are complex and raise specific privacy risks. In particular, there is the potential for financial services datasets to be combined to give a rich view of an individual's personal information, especially when considering the potential for cross-sector transfers between the energy and banking sectors. For example in the general insurance sector, the highly granular data available through the CDR would allow insurers to more easily distinguish between risks that may sometimes lead to negative outcomes for consumers, such as increased premiums or refusal of coverage.

The OAIC understands that the Treasury is committed to facilitating the conduct of additional Privacy Impact Assessments (PIAs) as the CDR system expands.[15] 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.[16] The OAIC supports this commitment and considers it will be important in light of any recommendations made by the Committee in relation to regulatory developments for the CDR system. The OAIC recommends that any future reports or recommendations of the Committee could identify and highlight the key privacy risks raised by stakeholders, that may be associated with any rollout of the CDR to relevant financial services sectors to ensure that steps are embedded to address the relevant risks in the design stages. This will assist with the conduct of future PIAs for CDR developments.

Interaction of CDR with international developments

The Issues Paper by the Committee is seeking feedback on the potential for Australia's CDR to interact with open banking data sharing schemes in other jurisdictions (e.g. California, the United Kingdom and Singapore), and how this potential can be realised.

The OAIC appreciates that today's global digital economy relies on data being able to flow securely and efficiently across borders. At the same time, cross-border data flows are subject to increased concern and

[15] The Agency response to the Consumer Data Right PIA (December 2019) supported a key recommendation by Maddocks that further PIAs may be necessary as various components of the CDR are revised or extended.

[16] Further, section 12 of the *Privacy (Australian Government Agencies – Governance) APP Code 2017* requires agencies subject to the Privacy Act 1988 (Privacy Act) to conduct a PIA for all 'high privacy risk' initiatives that involve new or changed ways of handling personal information.

scrutiny around the world.[17] It is therefore critical that any interaction between Australia's CDR system, and data portability regimes in other jurisdictions is designed appropriately to ensure the efficient movement of data across borders while including strong protections for individuals' personal information. Global interoperability does not require all countries to have identical open banking frameworks - instead it allows for bridges to be built across frameworks that reflect the cultural, social and legal norms of their society. In the OAIC's view, these bridges should allow data to flow safely and efficiently, while ensuring that individuals' personal information or data is protected, wherever it flows.

By way of background, under the CDR system the framework for cross-border data flows is established in two ways:

- Privacy Safeguard 8 (s 56EK of the Competition and Consumer Act) provides that CDR data must not be disclosed to an overseas recipient unless the recipient is accredited under the CDR,[18] or is subject to an overseas law that provides substantially similar privacy protections. Where international privacy laws do not provide substantially similar protections to the Privacy Safeguards, the accredited person who discloses the CDR data remains liable for future breaches by those overseas entities.[19]

- Overseas entities may also be accredited under the CDR system (s 56CA(2) of the Competition and Consumer Act), so that consumers may wish for their data to be securely sent to an overseas provider to access products or services.

The CDR also operates with extraterritorial application in certain situations (under s 56AO of the Competition and Consumer Act) for example when CDR data is held outside Australia but an act or omission causes suffering or financial disadvantage to an Australian person.

The OAIC considers that the approach established under the CDR strikes an appropriate balance between allowing CDR data to flow overseas, whilst ensuring there are meaningful redress mechanisms available to Australian consumers. This is important to ensure that individuals' CDR data remains protected in situations where there is no extraterritorial jurisdiction in relation to the acts or practices of an overseas entity.

The OAIC also notes that overseas data flows are currently being considered more broadly in relation to the Privacy Act under the Privacy Act Review. Three examples of these mechanisms are contractual safeguards, certification and 'adequacy' or whitelists.

The Committee may wish to consider whether any recommendations from that broader review in relation to these mechanisms could be applied under the CDR (as both the CDR and Privacy Act frameworks allow for cross-border disclosure, where there is appropriate accountability or where other jurisdictions have comparable privacy protections to the Australian CDR).

---

[17] 92% of Australians are somewhat to very concerned about their data being sent overseas, see: OAIC's *Australian Community Attitudes to Privacy Survey 2020* (September 2020).

[18] Section 56CA(2) of the Competition and Consumer Act provides that an overseas entity may be accredited under the CDR system.

[19] Privacy Safeguard 8 also allows overseas disclosures where conditions specified in the CDR Rules are met. However, there are currently no CDR Rules made in relation to this safeguard, so an accredited data recipient cannot rely on this exception.