Australian Government

Office of the Australian Information Commissioner

Submission to the Statutory Review of the Consumer Data Right

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

27 May 2022

OAIC

Contents

Executive summary

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Issues Paper for the Statutory Review on the operation of the Consumer Data Right (the Review). The Review is required under s56GH of the *Competition and Consumer Act 2010* (the Act) and aims to consider whether the existing statutory framework supports the evolution of the Consumer Data Right (CDR) and is fit-for-purpose to realise the CDR's objectives.

By way of general comment, the OAIC considers the Review to be an important evaluative measure and an opportunity to ensure robustness of the privacy, confidentiality and accessibility features of the CDR framework. Further, the OAIC notes, in previous CDR consultations, key CDR stakeholders have said a balanced approach to safety, efficiency and innovation is necessary to realise the benefits to consumers and grow participation in the CDR.[1]

The Open Banking Review noted comments from a range of stakeholders about the importance of providing a way for consumers to share their financial data to access better banking products and services without compromising their security and privacy.[2] Consistent with these findings and the response to this Review, the OAIC believes consumer trust is central to the success of the CDR and the security and privacy safeguards embedded in the CDR framework are the fundamental pillars for building and maintaining that trust.

In this respect, based on our regulatory experience of the CDR the OAIC has identified the following principles as being key to ensuring the statutory framework continues to support the evolution of the CDR, so that it is fit-for-purpose to realise the CDR objectives:

- significant elements of the CDR framework should be located in the primary legislation
- elements of the system core to the CDR's consumer value proposition, such as the privacy and security safeguards, should not be derogated from unless it is reasonable, necessary and proportionate to the relevant policy objective and appropriate safeguards can be put in place to ensure privacy risks are mitigated to provide a substantially similar level of protection
- aim to minimise or prevent regulatory gaps that could result in adverse impacts to consumers in relation to privacy, security and consumer protection
- when considering changes to the CDR, consider the operation of the CDR and the *Privacy Act 1988* (Cth) to minimise regulatory impact to participants and privacy risks for consumers.

[1] Department of Treasury (Treasury), Review into Open Banking in Australia – Final Report, Treasury website, December 2017, accessed 26 May 2022, p.8; See Treasury, Government Response to the Inquiry into Future Directions for the Consumer Data Right, December 2021, Recommendation 1.1 of Part 6.

[2] Treasury, Review into Open Banking, pp 51-52.

Key Recommendations

In order to maintain the high standard of privacy and confidentiality protections within the CDR regulatory framework, which is central to the success of the CDR, the OAIC makes the following recommendations, which reflect on the Terms of Reference for the Review:

1. Consider prohibiting practices that have an adverse impact on privacy and security for consumers, such as screen scraping
2. Embed the Farrell principles (referred to below) explicitly within the Objects of the CDR, set out at s 56AA of the *Competition and Consumer Act 2010* (Cth) and amend s 56AD to require the Minister to consider and report on how the objects of the Act have been met when proposing to designate a sector
3. Amend s 56AE of the Act to require the Minister to consult with consumers and/or an industry body representing the interests of consumers when proposing to designate a sector
4. Limit the use of sector specific rules for particular parts of the economy to ensure an appropriate balance is maintained between consistency and flexibility for participants and consumers
5. Significant elements of the CDR framework should be located in the primary legislation
6. Those elements of the system that are core to the CDR's consumer value proposition, such as the privacy and security safeguards, are located in the enabling legislation as this will prevent deviation and ensure consistency with those core principles across sectors
7. Aim to minimise regulatory gaps that could result in adverse impacts to consumers in relation to privacy, security and consumer protection
8. Prescribe that unaccredited third parties in receipt of CDR data are subject to the Privacy Act in respect of their handling of CDR data
9. Where data sets may have an elevated impact on the privacy of individuals, they should be included only if the privacy impacts are 'reasonable, necessary and proportionate' to achieving the policy objectives of the CDR and appropriate safeguards can be put in place to ensure privacy risks are mitigated
10. Conduct another statutory review of the CDR system within the next 5 years.

Further discussion about these recommendations is set out in the submission.

The privacy and security framework in the CDR

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.[3] A strong privacy and security framework is necessary not only for protecting consumers' information, but also for maintaining public confidence in, and the integrity of, the CDR scheme.[4]

The CDR has a strong privacy framework, and the Review is an opportunity to recognise where the CDR is working well to support participants to engage with the CDR system; protect the privacy and confidentiality of personal information, and promote trust and confidence in the CDR. In many ways, the CDR's privacy and security settings, consent model and accreditation is the gold standard for data sharing in Australia. The Review presents an opportunity to maintain the robust data protection and privacy framework and to embed these standards in the digital economy.

These privacy standards can operate as a benchmark for privacy settings in other contexts including the *Privacy Act 1988* (Cth) (Privacy Act). While the CDR privacy safeguards are new to both businesses and consumers now, the OAIC is committed to supporting businesses and consumers with detailed advice and guidance about the privacy settings. Supporting CDR participants will encourage consumers to confidently engage with the CDR knowing the appropriate protections are in place to keep their data secure; and businesses to be innovative and competitive participants in the CDR, so that consumers and businesses can confidently realise the benefits of greater competition and product innovation. Strong and consistent privacy and security settings are critical to making the CDR 'fit for purpose'.

Prohibition of unsafe practices

The OAIC's submission to the Inquiry into the Future Directions of the Consumer Data Right (Future Directions Inquiry) noted the prohibition of unsafe online practices, such as screen scraping by non-accredited third parties, in the UK and EU, suggesting consideration be given to how this may be leveraged to assist with future developments in the CDR.[5]

The practice of screen scraping presents a significant privacy and security risk to individuals which is at odds with the foundational security and privacy principles of the CDR. As suggested in the Financial Rights Legal Centre (FRLC) and the Consumer Action Law Centre's (CALC) submission to the Select Committee on Financial Technology and Regulatory Technology (Select Committee on Finance Technology,[6] allowing screen scraping to continue alongside the faster, safer data transfer mechanism under the CDR's Open Banking has the potential to undermine the success of the CDR regime. The FRLC and CALC note that unless screen scraping is prohibited, *'two very distinct FinTech sectors will be created: a sector that*

[3] Office of the Australian Information Commissioner (OAIC), Inquiry into Future Directions for the Consumer Data Right – Submission to Treasury, OAIC website, 21 May 2020, accessed 26 May 2022.

[4] OAIC, Consumer Data Right (CDR) exposure draft legislation — Submission to Treasury, OAIC website, 1 September 2018. accessed 26 May 2022.

[5] OAIC, Inquiry into Future Directions for the Consumer Data Right – Submission to Treasury.

[6] Financial Rights Legal Centre (FRLC) and Consumer Action Law Centre (CALC), Joint submission to the Senate Select Committee on Financial Technology and Regulatory Technology (FRLC and CALC Submission), FRLC website, December 2019, accessed 26 May 2022, pp17-18.

will adhere to higher privacy safeguards and standards and a sector that will not'.[7] Further, as noted in its submission to the same committee,[8] cyber security firm CyberCX stated that, rather than instilling in individuals an awareness of the importance of online security, encouraging people to reveal their passwords through screen scraping practices sends precisely the wrong message.[9]

The OAIC acknowledges that, given its wide range of applications, it is possible there may be some acceptable use cases for screen scraping, for example, internal operational reasons such as system migration. However, the OAIC recommends consideration be given to prohibiting the practice in circumstances where safer and more secure mechanisms for sharing personal information, such as the CDR, are available. This is consistent with the intent of the CDR to enable users to share information safety and efficiently. Further, prohibiting the practice of screen scraping has the potential to incentivise engagement with the CDR.

Recommendation 1: Consider prohibiting practices that have an adverse impact on privacy and security for consumers, such as screen scraping.

Objects in Part IVD

The objects of Part IVD, set out at s 56AA of the Act, are focussed on:

(a) enabling consumers to access and direct their information to be disclosed to accredited persons safely efficiently and conveniently
(b) enabling general access to information about goods or services where the information does not tend to identify consumers
(c) creating choice and competition or otherwise promote the public interest.

The OAIC considers the objects of the Act are relevant and fit-for-purpose. However, the objects of Part IVD could be strengthened by incorporating the principles set out in the Farrell Review into Open Banking. For example, referencing the principles that CDR is consumer focussed and that it must be efficient, fair and effective with security and privacy in mind.[10] Further , to ensure the Farrell principles remain embedded in the CDR, the OAIC recommends updating the matters the Minister must consider in s 56AD of the Act to require the Minister to

[7] FRLC and CALC, Joint submission to the Senate Select Committee, p 17.

[8] CyberCX, CyberCX submission to the Senate Select Committee on Financial Technology and Regulatory Technology Parliament of Australia website, December 2019, accessed 26 May 2022, p 5.

[9] CyberCX is led by CEO John Paitaridis and Chief Strategy Officer Alastair MacGibbon. Mr MacGibbon was recently National Cyber Security Adviser, head of the Australian Cyber Security Centre (Australian Signals Directorate) and Special Adviser to the Prime Minister on Cyber Security.

[10] Treasury, Review into Open Banking in Australia – Final Report, p. v.

also consider and report on how the objects in the Act are met when proposing to designate a sector.

Consultation

Consultation and clear communication between CDR agencies, targeted stakeholders and the public is essential for the success of the CDR in meeting the objects of Part IVD.

Consultation is imposed under the Act in a range of circumstances. For example, prior to the designation of a sector by the Minister, the Secretary of the Department must arrange for analysis of matters set out in s56AD(1)(a)-(e) of the Act and then undertake consultation with the general public,[11] the Australian Competition and Consumer Commission (ACCC), the Information Commissioner and the primary regulator of the sector that the instrument would designate.[12] The Minister must also consider a range of factors prior to making a designation, including the impact the designation will have on the privacy of individuals and confidentiality of business consumers.[13]

The OAIC considers the consultation obligations in the Act could be strengthened by requiring the Department to consult with consumers or consumer advocates. The present obligation to consult with the general public does not require specific consultation with consumers or consumer groups. While it would be open to consumer groups to participate in a public consultation process, noting the complexity of the CDR and the current level of consumer take up, the potential for in-depth engagement by consumer groups in a public consultation process is likely to be limited.

The interests of consumers, and the ability to understand the impacts on individuals of changes to the CDR system, may be better served by incorporating a specific requirement under the Act for engagement with a consumer advocate body that is appropriately resourced to consider and engage meaningfully with the issues.[14] Noting the complexity of the CDR and the issues involved, the Review may wish to consider whether funding could be allocated to enable the relevant body to perform this role. Access to consumer-focussed consultation and feedback of this nature would help inform the OAIC's advice to government as the CDR develops, as new sectors are designated and use of the system expands. In addition, expanding consultation to specifically include a consumer voice would also better align Part IVD of the Act with the objects at s 56AA and the emphasis on customer focus discussed in the Farrell Open Banking Review.

Consultation should be an agile and continuous process that enables learnings to feed into and improve the CDR system, for example, at the rule making and the designation stage.

---

[11] s56AE(1)(b) of the Competition and Consumer Act 2010 (Cth)(the Act).

[12] s56AE(1)(c) of the Act.

[13] ss56AD(1)(a)(iii) and 56AD(3) of the Act.

Recommendation 2: Embed the Farrell principles explicitly within the Objects of the CDR, set out at s56AA in Part IVD of the *Competition and Consumer Act 2010* (Cth) and amend s 56AD to require the Minister to consider and report on how the objects of the Act are met when proposing to designate a sector.

Recommendation 3: Amend s 56AE of the Act to require the Minister to consult with consumers and/or an industry body representing the interests of consumers when proposing to designate a sector.

Existing CDR framework (assessment, designation, rule-making and standard setting)

The CDR is a globally unprecedented framework that has been designed to engage cross-sector datasets, data holders and data recipients. As a result of this, the CDR regulatory framework is multifaceted and can appear complex. The CDR regulatory framework comprises Part IVD of the Act, the Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules), the Competition and Consumer Regulations 2010 (Cth) (CDR Regulations), designation instruments and various data standards, and all have a key role to play in framing and regulating the CDR.

Given the scope of the CDR, by design there is inherent complexity associated with operating the various legislative levers required to properly and safely implement the CDR across different sectors and datasets of the economy. The interaction and potential overlap between industry-specific consumer protections measures and the CDR regime was noted in the Final Report to the Inquiry into Future Directions. It was specifically noted that this should be considered when assessing the potential to designate a sector for data sharing or action initiation, with any barriers or conflicts between the regimes appropriately resolved.[15]

Role of primary legislation

While sector-specific rules provide an important opportunity to calibrate the CDR principles to particular parts of the economy, it means there is an increased risk of divergence that could result in the loss of the core CDR value proposition for consumers. The framework will better support future implementation where continuity of obligations across the rules is maintained, unless it is necessary to derogate in order to address a specific (sectoral) risk that may arise. However, ultimately it is the responsibility of the agencies to give the interface of simplicity for data holders and consumers.

[15] Treasury, Government Response to the Inquiry into Future Directions for the Consumer Data Right, Treasury website, December 2021, accessed 26 May 2022, Recommendation 7.1.

The OAIC has consistently recommended,[16] where possible significant elements of the CDR framework such as the privacy requirements should be included in primary legislation to guard against inadvertent or unforeseen risks to privacy. These may include the collection, use or disclosure of personal information that may not have been originally intended, known as 'function creep', or that which may not be reasonable, necessary and proportionate to the relevant policy objectives. To that extent, the OAIC recommends those elements of the system that are core to the CDR's consumer value proposition, such as the privacy and security safeguards, are located in the enabling legislation as this will prevent deviation and ensure consistency with those core principles across sectors. For example, the key requirements for a valid request and for CDR consents are important elements of the CDR privacy framework and apply to all CDR participants. At present most of the detail of these elements is included in the CDR rules rather than the Act.

CDR expansion and privacy protections

When considering changes to the CDR system, the OAIC recommends a cautious approach where those changes could impose additional privacy or security risks. This could arise, for example, in less mature sectors or from disclosure of CDR data to unaccredited entities where existing privacy legislation will not provide protections and the risk of a data breach could undermine confidence in the CDR system. The OAIC had previously highlighted this risk when consulted about the introduction of 'trusted advisers' in the CDR system and recommended that CDR data only be provided to trusted advisers where they are subject to the Privacy Act.[17] In that submission, the OAIC also noted that prescribed trusted advisers, such as those in the legal, accounting and management services and the finance industries are included in the top 5 industry sectors reporting data breaches to the OAIC.[18]

It is crucial to maintain strong privacy protections as the CDR expands and new participation pathways are introduced. The Privacy Act provides a mechanism to enable entities to be prescribed entities when handling personal information in specific circumstances. This minimises regulatory gaps and ensures personal information remains protected.[19]

A strong privacy framework will protect the rights of CDR consumers and build trust in the CDR. The Inquiry into Future Directions for the CDR noted consumers must be confident their rights will be protected when using the CDR as this will build consumer trust which is critical to the future success of the CDR.[20] These are important issues to keep in mind when

---

[16] OAIC, Trusted Digital Identity Bill legislative package: exposure draft consultation, OAIC website, 27 October 2021, accessed 26 May 2022, para 16.

[17] OAIC, OAIC Submission to Treasury's CDR Rules Amendments (Version 3) Consultation, OAIC website, 30 July 2021, accessed 26 May 2022.

[18] OAIC, Notifiable Data Breach report July to December 2020, OAIC website, 28 January 2021, accessed 26 May 2022, p6

[19] For example, 'reporting entities' are prescribed in s6E of the *Privacy Act 1988* in relation to their handling of personal information in relation to Anti-Money Laundering and Counter Terrorism Financing.

[20] Treasury, Inquiry into Future Directions for the Consumer Data Right – Issues Paper, Treasury website, March 2020, accessed 27 May 2022, p147

considering whether the existing assessment, designation, rule-making and standard setting requirements of the CDR support future implementation of the CDR including to government-held datasets. Further, careful consideration of these issues will ensure the key principles identified by Farrell are appropriately balanced between innovation and competition and consumer benefit and protection.[21]

Recommendation 4: Limit the use of sector specific rules for particular parts of the economy to ensure an appropriate balance is maintained between consistency and flexibility for participants and consumers.

Recommendation 5: Significant elements of the CDR framework should be located in the primary legislation.

Recommendation 6: Those elements of the system that are core to the CDR's consumer value proposition, such as the privacy and security safeguards, are reflected in the enabling legislation as this will prevent deviation and ensure consistency with those core principles across sectors.

Recommendation 7: Aim to minimise regulatory gaps that could result in adverse impacts to consumers in relation to privacy, security and consumer protection.

Recommendation 8: Prescribe that unaccredited third parties in receipt of CDR data are subject to the Privacy Act in respect of their handling of CDR data.

Operation and statutory settings of the CDR

The Review should consider whether the CDR regulatory framework in its current format can be easily understood and operationalised for participating entities. Any future changes to CDR regulatory framework should be considered in light of evidence gathered from stakeholders on the operation of the system in practice and the degree to which the system has benefitted participants by enabling improved product offerings and improved access to and control of information.

We have noted earlier in this submission that some level of complexity in the CDR is unavoidable. However, to the extent possible, the aim should be to reduce complexity and unintended consequences that impact on the integrity, privacy and security of the CDR system. The OAIC has a key role to play in assisting CDR participants to understand and implement their obligations and to collaborate with CDR agencies to support the rollout of the CDR. However, as the CDR continues to rollout across the economy it is important to ensure the CDR regulatory framework is functional for CDR participants to operationalise and for CDR agencies to regulate. This will build confidence and trust in both participants and

[21] Treasury, Review into Open Banking in Australia – Final Report, Foreword p .v.

consumers.

The expansion of the CDR to other sectors of the economy has the potential to benefit from:

- Creating a positive public narrative derived from high levels of consumer engagement with CDR in participating sectors, driving consumer demand for further sectors
- Understanding and learning from the implementation of CDR in one or some sectors through, for example, considering the risks and insights gained from participants during development of the Rules and Customer Experience (CX) standards, customer enquiries and complaints and assessment of compliance
- Giving businesses time to normalise the changes into business as usual (BAU), and start to realise the benefits of CDR
- Addressing the risks (including privacy risks) that have potential to undermine public confidence in the system
- Adjusting the regulatory settings accordingly.

Clarity is important when approaching the expansion of the CDR into new sectors and datasets. For example, the expansion of the CDR into government datasets reframes the previous CDR narrative and needs to be accompanied by assurance that the CDR 'brand' principles, including privacy and security and consent, will continue to apply. The OAIC has noted previously, privacy risks can be heightened in relation to government-held personal information because, amongst other things, government-held data is often acquired on a compulsory basis and may include information that is sensitive to the individual.[22]

Where data sets may have an elevated impact on the privacy of individuals, the OAIC recommends they should be included only if the privacy impacts are 'reasonable, necessary and proportionate' to achieving the policy objectives of the CDR and appropriate safeguards can be put in place to ensure privacy risks are mitigated.[23]

Continuing to ensure the initial intent of the legislation is pursued will provide clarity and confidence to consumers when engaging with the CDR and provide clear signals to participants about their role in maintaining the integrity of the CDR as it expands and grows.

Recommendation 9: Where data sets may have an elevated impact on the privacy of individuals, they should be included only if the privacy impacts are 'reasonable, necessary and proportionate' to achieving the policy objectives of the CDR and appropriate safeguards can be put in place to ensure privacy risks are mitigated.

[22] This does not necessarily mean it is sensitive information as defined in the *Privacy Act 1988* (Cth) but may become sensitive information when linked with other data.

[23] OAIC, Inquiry into Future Directions for the Consumer Data Right – Submission to Treasury.

Direct to consumer data sharing and Future focus

As the CDR continues to expand into new datasets and sectors, it is critical that robust privacy and confidentiality protections, underpinned by the above principles, continue to be maintained. The OAIC notes feedback to the review is likely to be reflective of the fact that the CDR system is relatively new, participant involvement is at the implementation phase and consumer engagement is low. This means is it difficult to assess what changes are necessary to the CDR framework at this point. One such example is direct to consumer data sharing.

The OAIC notes the Review is seeking input on whether Part IVD of the Act should be revised with respect to direct to-consumer data sharing. Providing consumers with increased access to their own data is consistent with fundamental privacy principles[24]. Further consideration needs to be given to the potential benefits and risks of enabling direct to consumer data sharing in machine readable form. This would allow data shared via an application programming interface (API) enabled for machine-to-machine communication, potentially enabling a consumer to use their data in an online service or tool. At present, a mechanism for consumers to access their personal information already exists under Australian Privacy Principle 12. Noting the level of consumer uptake for CDR, and the lack of information around use cases and privacy and security risks associated with this sort of data sharing, it would appear that additional time is required to properly assess the benefits.

This is just one example that illustrates how further maturity in the system would provide intelligence to assess the effectiveness and appropriateness of the CDR framework. With this in mind, the OAIC recommends that another statutory review of the CDR system is conducted within the next 5 years.

Recommendation 10: conduct another statutory review of the CDR system within the next 5 years.

[24] Treasury, Inquiry into Future Directions for the Consumer Data Right – Issues Paper, Treasury website, March 2020, accessed 26 May 2022.