Australian Government

Office of the Australian Information Commissioner

Consumer Data Right Strategic Assessment Consultation Paper

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

2 September 2021

OAIC

Contents

Overview

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the 'Implementation of an economy-wide Consumer Data Right - Strategic Assessment' consultation paper (consultation paper). We understand the responses to the consultation paper will inform Treasury's analysis and advice to the Minister following the Strategic Assessment regarding how the Consumer Data Right (CDR) should be implemented across the economy.

The consultation paper seeks views on how sectors and datasets should be prioritised and sequenced for roll-out, including information on the datasets or potential use cases that would deliver significant benefits to consumers and enhance competition and innovation. The consultation paper also seeks to understand:

- any sectors or datasets that may present elevated privacy concerns
- whether the CDR presents an opportunity to improve data sharing practices in these areas or otherwise address these existing privacy concerns, and
- where CDR may be particularly detrimental to the privacy of individuals.[1]

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 Rules) and advises Treasury, the ACCC and Data Standards Body on the privacy implications of the CDR legislation, rules and data 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.

The functions of the Australian Information Commissioner (Commissioner) include examining proposed enactments that may have an adverse effect on the privacy of individuals and minimising such effects.[2] In addition, under Part IVD of the *Competition and Consumer Act 2010* (Competition and Consumer Act), the Commissioner must also be consulted before a sectoral designation instrument is made, on the likely effect that making the instrument may have on the privacy or confidentiality of consumers' information.[3]

The OAIC makes this submission to provide our initial views on the sectors and datasets that may have elevated privacy risks for individuals and how any adverse effects may be minimised.

By way of overall comment, the OAIC is broadly supportive of the strategic vision for the CDR set out in the consultation paper,[4] which aims to facilitate an accelerated economy wide CDR roll-out to deliver benefits to consumers and drive innovation and competition.

We note that the expansion of the CDR into new sectors will have significant implications for the handling of consumers' personal information. In particular, the future sector roll-out will lead to increased data flows across and within sectors, with new potential for inherently sensitive datasets to

[1] Page 17 of the consultation paper.

[2] See s 28A(2)(a) of the Privacy Act, which outlines the 'monitoring related functions' of the Commissioner including in relation to the examination of proposed enactments.

[3] See s 56AD(3) Competition and Consumer Act.

[4] Page 8 of the consultation paper.

be combined and to provide richer insights about individuals. This may create opportunities for innovation and consumer benefit, but also give rise to increased privacy risk.

The Strategic Assessment will therefore require early consideration of the key privacy implications and risks associated with potential datasets and sectors being considered for designation. In this regard, the OAIC strongly supports the inclusion of 'privacy and confidentiality of consumer information' as a key Sectoral Assessment Criteria.[5]

Where elevated privacy risks are identified, consideration should be given during the prioritisation process as to whether, on the basis of the available evidence, any adverse effects on the privacy of individuals are reasonable, necessary and proportionate to achieving the CDR's policy objectives. Consideration should also be given to whether these impacts can be minimised and mitigated to an appropriate extent. Having a strong focus on privacy risks during the Strategic Assessment will be important for ensuring the CDR continues to be rolled-out in a way that achieves its core policy objectives and maintains public confidence in the integrity of the CDR system.

The OAIC understands Treasury is committed to facilitating the conduct of a Privacy Impact Assessment (PIA) during each statutory sectoral designation process, before any particular sector or dataset is designated.[6]The OAIC supports this commitment, noting it will be important to highlight the key privacy risks associated with any particular sector or dataset as early as possible. This will help to ensure that appropriate steps are taken during the sectoral assessment and implementation phases to minimise the adverse impacts on the privacy of individuals.

In addition, the OAIC notes that there are a number of data and privacy related streams of work underway across government[7]and it will be important to have visibility of this work during the Strategic Assessment to ensure these streams are moving in a complementary direction.

Comments on potential sectors and data sectors for designation

The consultation paper sets out potential sectors and datasets that may be suitable for designation under the CDR.[8] The OAIC understands that the prioritisation and sequencing of the CDR roll-out will be assessed with regard to the overarching policy objectives of the CDR to deliver consumer value, enhance competition and innovation, and promote secure data sharing practices.

The OAIC notes there are specific sectors and datasets raised in the consultation paper which are considered by the community to have increased levels of sensitivity and deserve additional protections. The OAIC provides a discussion below on examples of sectors or datasets that have elevated privacy risks including:

---

[5] Page 7 of the consultation paper.

[6] Page 17 of the consultation paper. 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.

[7] For example, the proposed Online Privacy Code, review of the *Privacy Act 1988*, the recently amended *Online Safety Act 2021* and proposed codes, the Data Availability and Transparency Bill 2020 and the Trusted Digital Identity Framework, in addition to implementation of Australia's Cyber Security Strategy 2020.

[8] Potential future sectors outlined in the paper include: agriculture, general insurance, groceries, health, loyalty schemes, non-bank lenders, transport, superannuation, government, health insurance, education and digital platforms

- financial services
- digital platforms
- government, health and education data
- location data, and
- government identifiers.

In particular, when assessing the privacy risks of proposed sectors or datasets, it is important to consider whether consent alone provides sufficient protection. While the CDR framework contains strong privacy protections, a consent-based model may not be sufficient for certain use cases involving highly sensitive or complex datasets.[9] This is because consumers are not always well-placed to assess the risks and benefits of allowing their data to be shared and analysed in more complex circumstances. This risk increases with the sensitivity of the data, vulnerability of the customer, and alternate options or pathways available.

For example, when consumers consent to sharing their sensitive data, it may be difficult to understand what insights can be derived about them and what other information it may be combined with. The risks are magnified in circumstances where consumers may consider:

- they do not have a choice but to share their information as they are reliant on the products or services being offered by an accredited data recipient or
- they will not receive the same deal or offer if they do not share their information.

This is supported by studies that have found consumers tend to overvalue immediate benefits and costs (for example, the benefits of the good or service), while struggling to accurately assess more delayed benefits and costs such as privacy risks.[10]

We therefore recommend that Treasury takes a cautious approach to designating datasets with significant data sensitivities that may pose privacy risks for consumers, particularly vulnerable consumers. In particular, the OAIC advises against designating certain sectors and datasets with inherent sensitivities, such as the health insurance sector, digital platform data or location data, unless 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. Examples of additional protections include limits on what types of personal information an accredited data recipient is permitted to combine with CDR data, purpose limitations or prohibitions to ensure that CDR data is being used in a fair and reasonable way, or prohibitions on certain types of ADRs obtaining particular datasets.

As expected, at this stage the use cases or policy objectives for designating certain sectors and datasets are not developed, which makes it difficult to properly assess the risks to individual privacy posed by the proposed sectors and datasets or to weigh the potential benefits of designation against any inherent privacy risks. The OAIC therefore recommends that, where the strategic assessment process reveals potential use cases or objectives that will be further considered for possible designation, that further consultation is also undertaken on privacy risks. This will allow stakeholders

[9] For an overview of the limitations of consent, particularly in light of the various challenges and complexities created by digital technologies, see paragraph 5.18 of the OAIC's Submission to the Privacy Act Review – Issues Paper (December 2020).

[10] See discussion of bounded rationality at Taylor M & Paterson J (in press) Protecting privacy in India: The role of consent and fairness in data protection Indian Journal of Law and Technology, p. 18.

to provide targeted comments about the privacy risks of the specific use cases, and whether this is reasonable, necessary and proportionate to the benefits that consumers might gain.

Financial services (superannuation, insurance and non-bank lending)

There has been considerable interest in designating the financial services industry, which includes superannuation and general insurance as well as non-bank lenders.[11] From a privacy and information access perspective, the OAIC is broadly supportive of the roll-out of the CDR to sectors in the financial services industry, as we recognise the potential benefits to consumers from having greater access to, and control over, their financial services data.

While many of the current CDR privacy settings may be appropriate for the broader financial services sector (as the privacy risks relating to the financial services industry share similarities with those in the banking sector), there will be additional and different privacy risks across the various parts of the financial services industry. These will need to be separately identified, analysed and mitigated. For example, in the general insurance sector, the highly granular data available through the CDR would allow insurers to more easily distinguish between risks which may lead to negative outcomes for consumers, such as increased premiums or refusal of coverage.

If the insurance sector is identified as a priority sector for designation, the OAIC recommends that there be a carve out to explicitly exclude particular datasets held by the health insurance sector. This is because there are highly sensitive datasets and existing regulatory restrictions specific to the health insurance sector that render particular data sets as unsuitable for designation.[12] Health insurers are highly regulated regarding how they can use personal information to rate risk. For example, the *Private Health Insurance Act 2007* requires health insurers to charge everyone the same premium for the same product, and prevents them from charging different premiums based on past or likely future health, claims history and age, pre-existing condition, gender, race or lifestyle. The OAIC also notes that the *My Health Records Act 2012* contains a specific prohibition against using information contained in an individual's My Health Records for insurance purposes. Designating highly sensitive health insurance datasets (such as claims information) would raise privacy risks by allowing this data to flow to recipients acting outside of the highly regulated health insurance sector, potentially allowing this data to be used contrary to the regulatory framework that currently protects that data.

Digital Platforms

The consultation paper contemplates digital platforms as a potential future sector for roll-out under the CDR.

The OAIC has found significant community concern about the data handling activities of digital platforms. For example, the OAIC's 2020 Australian Community Attitudes to Privacy Survey found that:

---

[11] For example, designating the financial services sector was recommended in the Inquiry into Future Directions for the CDR Final Report and the Select Committee on Financial Technology and Regulatory Technology.

[12] *My Health Records Act 2012* (Cth), s 70A.

- Australians consider the social media industry the most untrustworthy in how they protect or use personal information (with 70% considering this industry untrustworthy)
- over half of the individuals surveyed expressed discomfort with digital platforms tracking their location through their browser (62%) and targeting advertising based on their online activities (58%).

In addition, the OAIC notes that there have been a range of inquiries that have examined the privacy and consumer harms that may arise from the data handling activities of digital platforms. For example, the ACCC's Digital Platform Inquiry identified a range of potential consumer harms that may arise from the collection, use and disclosure of personal information by digital platforms. These include issues relating to unsolicited targeted advertising, potential discrimination or exclusionary practices which target vulnerable consumers based on attributes from their material online.[13]

The Select Committee on Australia as a Technology and Financial Centre's second interim report also noted evidence provided by the OAIC, that participation by digital platforms in the CDR may raise a range of significant privacy risks. For example, that due to the volume of data held by these entities, digital platform participation in the CDR would allow these entities to build profiles of individual consumers, and to derive and provide deep and rich insights into those individuals. Given the reach of digital platforms, and their 'track record' of using data in ways that may not meet community expectations, the Committee recommended that consideration be given to what additional safeguards may be required in the event that large non-bank digital platforms were to seek accreditation.[14]

While the above comments and findings were made in the context of digital platforms seeking accreditation, the OAIC considers these concerns are also relevant in the context of designating digital platforms or the datasets they hold. Given the sensitivity and consumer harms that could potentially arise from the sharing of this data, the OAIC recommends against considering digital platforms or their datasets for designation under the CDR, unless compelling, narrowly defined use cases with significant consumer benefit are identified. If there are compelling use cases with significant consumer benefit for designating digital platforms data, the OAIC recommends that Treasury consider whether there should be further prohibitions on how this data is used in certain circumstances to prevent potential consumer harms that may arise. For example, whether there should be limits on the types of digital platform data that accredited persons should have access to, or whether there should be a prohibition on combining digital platform data with sensitive data that is already held by the entity.

Government, health and education data

The consultation paper seeks views on including the government, health and education sectors as a potential future sector.

In relation to government held data, the OAIC notes that the information environment in relation to government entities can differ compared to private sector entities. Privacy risks can be heightened in relation to Government-held personal information, which is often collected on a compulsory basis

[13] ACCC Digital Platforms Inquiry Final Report 2019, Chapter 7.3-7.4.

[14] The Select Committee on Australia as a Technology and Financial Centre Second Interim Report, April 2021, Recommendation 5.

under a law such as the *Income Tax Assessment Act 1936*, or to enable individuals to receive a statutory entitlement, government benefit or grant considered to be essential by the individual. Such data is often sensitive or can become sensitive when it is linked with other datasets. This may impact vulnerable consumers using the CDR in particular, as their information is more likely to be included in such datasets, they may feel reliant on government services or payments and may feel a loss of control over their personal information and unable to make meaningful choices about the collection, use and disclosure of their data. This calls into question whether consent is genuinely informed and voluntary. In addition, before considering designating government-held data, it will be important to carefully consider the policy intent behind the CDR and ensure there is a clear consumer benefit to including such datasets in this regime.

Regarding health data, the OAIC notes that this data is considered by the community to be highly sensitive, with the potential to give rise to discrimination against individuals.[15] In recognition of this sensitivity, the *Privacy Act 1988* (Privacy Act) provides extra protections around the handling of health information, such as generally requiring consent before an individuals' health information is collected. Similarly, regarding education data, data about children collected from educational institutions over many years enables a highly detailed picture to be created about young people from an early age, which can include health information, academic aptitude, and behavioural issues. The OAIC's 2020 Australian Community Attitudes to Privacy Survey also found that two thirds of parents are uncomfortable with businesses being able to obtain information about a child (such as age, location, and interests) where sensitive information can be inferred and used to target or profile them.

Given the sensitivity and nature of the data held in these sectors, we recommend that Treasury takes a cautious approach to designating these sectors and datasets.

Location data

The OAIC considers there are particular privacy risks associated with designating location data as a dataset for the CDR, as it can be used to profile individuals and reveal detailed insights in relation to a consumer.

Location data is particularly intrusive in that beyond showing where an individual has been, it can also reveal sensitive information about them such as information about their health or religious beliefs. There are additional complexities associated with products and services that commonly use geolocation data (for example phones and wearable trackers), where many of these products are 'always on' and connected to the internet by default. The seamless nature of how GPS technology is built into these devices means that consumers (and possibly other individuals in the consumer's network) are not fully aware of what personal information is collected, stored and shared, or what purposes this data is used for.

[15] See Australian Law Reform Commission(ALRC) (2008), *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, p. 319.

The OAIC's 2020 Australian Community Attitudes to Privacy Survey found that Australians are uncomfortable with the use of location tracking and the handling and use of that information. Half (48%) of Australians consider it is one of the biggest privacy risks today.[16]

Given the sensitivity of location data (both perceived and actual), the OAIC has recently recommended that in certain contexts, a full or partial prohibition on the handling of location data about individuals be introduced into the Privacy Act.[17]

Although location data is already held and used by digital platforms and telecommunication providers and while there may be competition and innovation benefits with making this data more widely available, there is also significant community concern with its use. The OAIC considers that designating an individual's location data for CDR and expanding the scope of entities who may access and use location data presents privacy or confidentiality risks that may not be able to be mitigated to the appropriate extent. The OAIC therefore recommends that location data should not be considered as a potential dataset for designation unless and until such time as the risks can be appropriately mitigated.

Government identifiers

The consultation paper also considers designating government identifier datasets such as passports. A government related identifier is an identifier that has been assigned by an agency, a State or Territory authority, an agent of an agency or authority, or a contracted service provider for a Commonwealth or State contract.

The OAIC notes that government identifiers raise heightened privacy concerns, that may make such datasets unsuitable for CDR designation. Government related identifiers are currently provided additional protection under the Australian Privacy Principles (APPs) in the Privacy Act and the CDR Privacy Safeguards in the Competition and Consumer Act to ensure they are not adopted, used or disclosed by other entities and therefore become universal identifiers.[18] The OAIC considers that if government related identifiers were to become designated datasets under the CDR to support innovative use cases across multiple sectors, this may give rise to a risk that these datasets are linked or matched with other datasets in ways beyond their original purpose, or in ways which a consumer does not expect. For example, they could potentially be used to centralise substantial amounts of information about consumers' behaviours and preferences.[19] The increased sharing of this information can also create security risks. If government related identifiers were subject to unauthorised disclosures, this would likely elevate the individual's risk of identity theft.

The OAIC therefore would generally recommend against the designation of government related identifiers such as passports, Medicare numbers and Centrelink numbers. In the event that a

---

[16] See the OAIC's 2020 Australian Community Attitudes to Privacy Survey.

[17] See Recommendation 40 on page 16 and commentary on page 42 of the OAIC's Submission to the Privacy Act Review – Issues Paper (December 2020).

[18] Australian Privacy Principle 9 restricts the adoption, use and disclosure of government related identifiers by APP entities unless an exception applies. Privacy Safeguard 9 sets out a prohibition on accredited data recipients of CDR data from adopting, using or disclosing government related identifiers unless an exception applies.

[19] See Australian Law Reform Commission (2008), *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, Australian Government, p. 1051.

compelling use case arises, close consideration would need to be given as to whether the privacy risks would be able to be sufficiently mitigated.