**Select Committee on Financial Technology and Regulatory Technology**
ANSWER TO QUESTION ON NOTICE

**Department/Agency:** Office of the Australian Information Commissioner
**Topic:** Large technology companies and the Consumer Data Right system
**Date:** 2 March 2021

**Question:**

**CHAIR:** That was very useful. That's something which we're looking at and we'll look at that closely. Please feel free to send anything else on notice on that if there's anything that you feel you'd like to add to your statement on that particular issue as we consider the question of whether or not there's a policy justification for a separate system, or a modified system.

**Answer:**

The Office of the Australian Information Commissioner (OAIC) is not aware of any large technology companies currently being accredited under the Consumer Data Right (CDR) system, or whether any such companies have an intention to participate. The below response is therefore general in nature.

As outlined by the OAIC in the recent public hearing and submission to the Committee, the Australian Competition and Consumer Commission's Digital Platforms Inquiry Final Report (Digital Platforms Inquiry) identified a wide range of consumer harms that may arise from the collection, use and disclosure of personal information by digital platforms.[1]

Based on the nature of the findings under the Digital Platforms Inquiry, a range of potential privacy risks could arise if large technology companies were to participate in the CDR system. The OAIC highlighted a number of these for the Committee in the public hearing. In particular, powerful insights may be able to be derived from an individual's CDR data when combined with other data held about them (including sensitive information), which could be used in ways the consumer might not expect.

The CDR system already has some strong privacy protections in place to mitigate some of the potential risks, including being a consent-based system, which provides consumers with the ability to exercise choice and control about how their data is handled.[2] There are also prohibitions on CDR data being used in certain circumstances.[3]

However, because of the rich data holdings of digital platforms, additional protections may be necessary to further protect consumers in circumstances where their CDR data may be combined with existing data held about them, such as from their social media profiles.

---

[1] See the OAIC's submission of 15 December 2020 to the Select Committee on Financial Technology and Regulatory Technology, available at www.oaic.gov.au/engage-with-us/submissions/select-committee-on-financial-technology-and-regulatory-technology.

[2] Division 4.3 of the *Competition and Consumer (Consumer Data Right) Rules 2020* (CDR Rules) requires that accredited data recipients may only collect, use (and in limited cases, disclose) CDR data with the consumer's express consent. Consumers must actively select which data they consent to being collected, and what specific uses they consent to (other than those which may be required or authorised by law). Consent is time-limited (maximum of 12 months) and must not be bundled with other directions, permissions, consent or agreements.

[3] See for example Privacy Safeguard 7 (s 56EJ of the *Competition and Consumer Act 2010*), which prohibits direct marketing, except in limited circumstances set out in the CDR Rules, and only where the consumer consents to it.

The OAIC therefore recommends that the Committee consider:

- whether there should be limits on what CDR data digital platforms should be able to access via the CDR system, and/or whether there should be limits on what existing personal information CDR data should be able to be combined with. For example, location data or 'sensitive information' (includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record),[4]
- whether any specific uses or disclosures of CDR data by a digital platform should be prohibited. For example, those uses or disclosures that relate to assessment of an individual's suitability for essential services such as housing or healthcare, or any employment-related purposes, and
- whether a fairness and reasonableness obligation should be introduced. For example, a requirement that any collections, uses and disclosures of CDR data must be fair and reasonable in the circumstances, even if a consumer consents to the collection. This would create a proactive obligation for accredited data recipients, aimed at preventing unfair and/or unreasonable uses of CDR data that may result in harms to individuals, or discriminatory outcomes.[5]

[4] 'Sensitive information' is defined under subsection 6(1) of the *Privacy Act 1988*.

[5] The OAIC has also recommended a fairness and reasonableness obligation for APP entities (Recommendation 37) in our submission to the Australian Government's review of the Privacy Act 1988, in response to its Issues Paper. The OAIC's submission is available at www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission.