Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D18/134144

12 October 2018

Ms Sarah Court
Commissioner
Australian Competition & Consumer Commission
GPO Box 3131
Canberra ACT 2601

Dear Ms Court,

Review of the ACCC Consumer Data Right Rules Framework

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission to the Australian Competition and Consumer Commission (**ACCC**) in relation to the review of the ACCC Consumer Data Right (**CDR**) Rules Framework (**the Framework**).

OVIC is the primary regulator for information privacy, data protection and freedom of information for the state of Victoria. As Information Commissioner I have a strong interest in matters that affect consumers' privacy, and one of my functions under the *Privacy and Data Protection Act 2014* (**PDP Act**) is to make public statements in relation to such matters.

This submission outlines my office's views on the Framework, in particular, the approach to consent that has been proposed under the Framework and the need for clarity and consistency around the proposed privacy safeguards.

Consent

1. The Framework sets out in detail a traditional notion of consent, where the onus is on the consumer to inform themselves of how their information will be handled before they make a decision to access a service. This responsibility ultimately increases the difficulty for consumers in choosing (where possible) whether to consent to share their data. Often consumers will not have an understanding of the implications of what they are consenting to, or the full range of contexts in which the consent will apply, and utilising notice and consent as a means of privacy assurance is not an approach that always effectvely prioritises the interests of the consumer. Consumers may feel compelled to provide their consent in order to access a service, despite not comprehending lengthy and technical conditions. As these terms can be difficult to understand, consumers are consequently discouraged from reading them, resulting in consent being provided in a way that is not meaningful or informed.

2. There has been a trend in the global privacy community to move away from a transactional model of consent towards establishing a minimum standard of protection. The *Treasury Laws Amendment (Consumer Data Right) Bill 2018* and the Framework detail several protections that reflect the modern approach to consent, such as the introduction of a consumer dashboard to review consents provided and the provision of consumer comprehension tested information "visually in

accordance with design best practices."[1] This is a great foundation for establishing a minimum standard, and there is room to further instil this baseline level of protection in the CDR regime's general approach to consent. Consent requirements under the European Union's General Data Protection Regulation (**GDPR**), and the privacy protections the GDPR offers more broadly, set an excellent minimum standard of protection.[2] Although it places consumer choice at the forefront, the heavy reliance the Framework places on consumer consent may not necessarily provide consumers with the highest standard of privacy protection.

3. Once a consumer's data becomes 'redundant data', best practice is to destroy information that is no longer relevant. Allowing consumers to choose how redundant data should be handled, either de-identified or destroyed, again places the responsibility on the consumer to educate themselves about each of these options in order to understand the associated privacy risks.[3] A consumer will likely not have the detailed understanding of these concepts and the implications of de-identification on their privacy to form, and act on, an informed view. Consent is not envisioned to be a catch-all mechanism, but rather a meaningful agreement based on clear, unambiguous information detailing what is being consented to and how the information may or may not be used. The onus should not be placed on the consumer to make an educated decision, where they may not be in a position to do so. A lack of technical understanding in this context may place the consumer at the risk of making an uninformed, and potentially detrimental, choice. Further, there are inherent risks involved in retaining data that is no longer required, even if it is de-identified, given the relative ease with which re-identification can occur.[4] OVIC is aware of multiple instances in which a poor understanding of the limits of de-identification has resulted in unintentional breaches of privacy. OVIC recommends that by default, data recipients be required to destroy redundant data under the Framework.

4. Allowing a consumer, albeit with notice from the data holder, to consent to provide their data to an unaccredited recipient raises similar issues. The responsibility is placed on the consumer to inform themselves of the trustworthiness of an unaccredited data recipient, and make a decision for themselves about whether they are willing to take on the risk of providing their information to a recipient who may not be bound by standards of privacy or data protection. The Framework states that, "(t)he CDR places the value of consumer data in the hands of the consumer",[5] and while OVIC agrees that allowing consumers the choice to move between providers is valuable, the risks to their information are inherently greater where the onus is on the consumer to take responsibility for its protection. Governance provisions may become meaningless if there are actors in the system that are not subject to the same level of oversight as accredited data recipients.

5. The question of whether a mature minor can lawfully provide consent is a complex area and continues to be examined by the courts.[6] Advising age ranges in which a minor is considered capable of providing consent may be too prescriptive, as determinations of a child's capacity to provide consent are subjective and depend on the individual minor. The ACCC could look to the results of the implementation of the GDPR over the coming years as a helpful guide to inform a view on the lawful consent of minors. It is likely that some trends will emerge in this area, prompted by the implementation of the GDPR, and for this reason OVIC suggests that minors be excluded from the initial formulation of the CDR. This will allow the ACCC to make an evidence based decision on this matter in the future, taking into account international learnings.

---

[1] Page 37 of the Framework.
[2] See, Articles 7 and 8 of the GDPR.
[3] On page 32 of the Framework.
[4] See OVIC's report on *Protecting unit-record level personal information* for a discussion on the risks of de-identifiation, available at https://ovic.vic.gov.au/wp-content/uploads/2018/07/Protecting-unit-record-level-personal-information.pdf.
[5] On page 48 of the Framework.
[6] See for example, *X v The Sydney Children's Hospitals Network* [2013] NSWCA 320; *Re Jamie* [2013] FamCACF 110; and *Central Queensland Hospital and Health Service v Q* [2016] QSC 89.

6. For a consumer to provide truly informed and freely given consent, it would be helpful for consumers to receive an explanation about the consequences should consent not be provided, and the alternatives available to them if they choose not to consent.[7] This is an important element in ensuring that consent is genuine rather than coerced, and provides some protection against pathways that nudge people to make choices without clear options. It is in the interests of data holders to provide more information to consumers in a clear and relatable way. The CDR regime is already taking positive steps towards establishing this, and elements to ensure free and informed consent should be incorporated into the existing Framework.

Clarity and consistency around privacy

7. The proposed Framework outlines 12 privacy safeguards that closely mirror the Australian Privacy Principles (**APPs**) set out in the Commonwealth *Privacy Act 1988*. However, the CDR privacy safeguards provide some additional protections and derogations from the APPs. In some cases, the safeguards will apply concurrently with the 13 APPs, while in others, the safeguards will only apply to specific data holders. The duplication of privacy protections is likely to confuse the privacy landscape for stakeholders; not only will data recipients be required to navigate two privacy regimes concurrently, but consumers are also likely to be unsure as to where their privacy rights stem from. For clarity, consistency and to ease the transition to the CDR regime, an alternative approach could be to apply the existing privacy rights and obligations under the APPs as they stand, with relevant additional protections and derogations for the CDR implemented as necessary under the Framework. Clarity and simplicity in developing and implementing the CDR is an important element that will not only benefit the consumers, but also assist data holders and accredited data recipients navigate the new CDR regime.

Auditing of accredited data recipients

8. To cement and support good governance practices, OVIC would suggest that auditing processes be implemented to ensure that all accredited data recipients are meeting the compliance requirements under the CDR. OVIC notes that any audit and oversight role the Office of the Australian Information Commissioner or the ACCC performs will be complemented by the requirements under the proposed CDR rules for data recipients to maintain records regarding their compliance with the privacy safeguards.[8]

Thank you for the opportunity to comment on the Framework. OVIC will continue to follow the progress of the CDR with interest.

I have no objection to this letter being published by the ACCC without further reference to me. I also propose to publish a copy of this letter on the OVIC website but would be happy to adjust the timing of this to allow the ACCC to collate and publish submissions proactively.

If you have any questions concerning the above, please contact Emily Arians, Senior Policy Analyst at emily.arians@ovic.vic.gov.au.

Yours sincerely,

Sven Bluemmel
Information Commissioner

[7] As noted on page 35 of the Framework.
[8] Page 59 of the Framework.