New Zealand Law Society
Te Kāhui Ture o Aotearoa

Level 4, 17–21 Whitmore Street, Wellington
PO Box 5041, Wellington 6140 · DX SP20202, Wellington
04 472 7837 · inquiries@lawsociety.org.nz

lawsociety.org.nz

9 October 2020

Consumer Data Right Project Team
Commerce, Consumers and Communications
Ministry of Business, Innovation & Employment
Wellington

By email: consumerdataright@mbie.govt.nz

Tēnā koe

Re: Options for establishing a consumer data right in New Zealand

The New Zealand Law Society | Te Kāhui Ture o Aotearoa (**Law Society**) welcomes the opportunity to comment on the Ministry of Business, Innovation and Employment (**MBIE**) discussion document *Options for establishing a consumer data right in New Zealand* (**discussion document**).

MBIE is considering whether to develop a consumer data right (**CDR**) in New Zealand "to give individuals and businesses greater choice and control over their data".[1] The discussion document contains a high level analysis of the options to establish a CDR in New Zealand, and more detailed analysis will be completed as part of the ongoing policy development process.

In light of this, the Law Society provides the following brief comments focussing on matters that may affect the workability of a statutory CDR. We have not responded to the specific consultation questions.

Overview of the options

The aim of a CDR is to give individuals and businesses greater choice and control over their data by allowing them to securely share data held about them by businesses such as a bank or utility with trusted third parties.[2] The discussion document sets out four main options for the high-level approach to designing a CDR:

1. Option 1: status quo – the government would not introduce a consumer data right and the development of consumer data portability would be left to individual businesses or sectors.
2. Option 2: a sectoral designation approach – a high-level framework would be established in legislation that would apply across the entire economy, but the CDR would only apply to sectors or markets that had been designated through secondary or tertiary legislation.
3. Option 3: an economy-wide CDR – data portability rights would be set out in legislation.
4. Option 4: sector-specific approach – distinct CDRs could be designed for specific sectors as the need arose including sector-specific legislation.

---

1 Ministry of Business, Innovation and Employment, Discussion Document, *Options for establishing a consumer data in New Zealand*, at [1].

2 Ibid, at [7].

Should a CDR be established, the discussion document considers Option 2 is the appropriate vehicle for designing a CDR, including considering how a legislative framework would intersect competition, consumer and privacy laws.

Whichever option is selected, a choice will need to be made about whether to create a new, specific statute, or whether to locate the right within an existing statute. MBIE's preliminary view is that a CDR may sit better as a stand-alone Act.[3]

Should the CDR be located in the Privacy Act 2020?

If a CDR is to be located within an existing statute, the most obvious option is the Privacy Act 2020 (**Privacy Act**). In that Act, Information Privacy Principle 6 contains a consumer right to request and obtain access to information about the requester.[4] It also governs when that information should be made available, and the form in which it should be made available. Any CDR is effectively an extension of that existing right of access.

As noted in the discussion document, the European Union's General Data Protection Regulation (GDPR) similarly contains a 'data portability' right.[5] In addition, the New Zealand Privacy Commissioner has submitted that the right would be a valuable addition to the Privacy Act.[6] Therefore, including a CDR within the Privacy Act is a valid and workable option.

However, a CDR in this context would be limited to personal information about the requestor. As noted in the discussion document, a CDR can also be seen as a right focused on a desire to increase competition, either in specific markets or more generally.[7] If competition, rather than privacy, is the main policy driver for introducing a CDR, we agree with MBIE's view that a CDR might go beyond information that is about the requester. For instance, it could include a more general obligation on organisations to be transparent about their products and services. Therefore, the more a CDR is extended beyond just 'personal information', the more conceptually confusing it would be to include a CDR in the Privacy Act.

An alternative CDR statutory framework?

General comments

If a CDR is to be located outside the Privacy Act, the new statute would need to clearly set out how its provisions intersect with Privacy Act provisions – including, for example, how a CDR might affect

---

3 Ibid, at [63].

4 Information Privacy Principle 6 states: "An individual is entitled to receive from an agency upon request—
(a) confirmation of whether the agency holds any personal information about them; and (b) access to their personal information. If an individual concerned is given access to personal information, the individual must be advised that, under IPP 7, the individual may request the correction of that information…".

5 Above n 1, at [8]. As noted in the discussion document, the GDPR "gives individuals the right to receive a copy of their personal data in a structured, commonly used and machine-readable format and transfer this data to a trusted third party", at p 8.

6 See for example the Privacy Commissioner's submission on the Privacy Bill at 1.9(b) where the Privacy Commissioner recommended the Act be amended to include "a right to personal information portability – bolstering the right of individuals to access their own personal information by including "data portability" as a right for consumers to transfer their personal information to another service provider".

7 The discussion document highlights perceived benefits of a CDR including the introduction of new products and services which will increase competition and innovation, at [10].

the ability to request the same information under the Privacy Act. This is to ensure there is no confusion about the correct interpretation of the law around data portability, and to reduce the risk of parallel complaints procedures.

Types of information – provided data and derived data

MBIE have suggested that only 'provided' or 'observed' data would be subject to the CDR and 'derived' data[8] should generally be excluded from the definition of 'consumer data',[9] given it may be commercially sensitive. However, MBIE also acknowledge that derived data may still be considered 'personal information' for the purposes of the Privacy Act and individuals could therefore request that information under the Privacy Act.[10]

Section 24 of the Privacy Act expressly acknowledges that other legislation may override the principles of the Act. Consequently, it would be possible to specify that the Privacy Act did not apply to any personal information that was covered by the relevant CDR provisions.

However, the Human Rights Review Tribunal has been clear that it will be slow to read down the Privacy Act principles. If the law is ambiguous, the Act will continue to operate.[11] If a new legislative framework is established, the CDR provisions will need to clearly state the types of information that are covered, and the extent of any Privacy Act override.

If, as indicated by MBIE, 'derived' data was omitted from a CDR (because it is likely to give rise to arguments about commercial confidentiality or trade secrets), we agree that 'derived' data may in many cases still be personal information that the person is entitled to request under the Privacy Act – and, if the commercial argument is not strong enough, or the public interest is significant, the information may have to be released.

It is therefore possible that individuals may make requests under both statutory frameworks (i.e. any new CDR framework and the Privacy Act) and they might theoretically be entitled to receive further information through the Privacy Act route. If that happens, several other factors will need to be considered, including for example, how a CDR might affect the interpretation of section 52 of the Privacy Act, which protects trade secrets and commercially sensitive information (especially as that protection is subject to any overriding public interest in making the information available).

Excluding 'derived' data without more clarity about what that means in practice, risks shifting the argument about the strength of any commercial interest for protecting the 'derived' data, to the Privacy Act which contain separate complaints and enforcement processes.

We invite MBIE to consider these issues in more detail.

Access to enforcement processes

The discussion document does not deal in any depth with the issue of enforcement processes for a CDR, but enforcement options are likely to have a significant impact on the choice of legislative vehicle for establishing a CDR.

The Privacy Act already provides a clear existing enforcement regime, with complaints determined by the Privacy Commissioner and a subsequent ability to go to the Human Rights Review Tribunal.[12]

---

8 Data that has been created by a data holder through the application of insights and analytics.

9 Above n 1, at [20].

10 Ibid.

11 See *Andrews v Commissioner of Police* [2013] NZHRRT 6, 4 March 2013, at [53].

12 Privacy Act 2020, part 5.

These processes are free for consumers. If a CDR is established as an extension of the right to access personal information, it could also be included in the Privacy Commissioner's new power to issue binding access directions (with a right of appeal to the Human Rights Review Tribunal).[13] This would provide a clear, enforceable and relatively swift first instance decision on whether the right operates in any given circumstances.

Alternatively, if a CDR is established under stand-alone legislation, a new complaints and enforcement mechanism would need to be developed. While it may be possible to use some form of existing industry scheme to resolve complaints, there may be jurisdictional issues and not all schemes result in binding determinations. Any requirement for consumers to go to court to enforce their rights would undermine the effectiveness of the right: such an avenue is expensive and time-consuming.

Conclusion

We appreciate the opportunity to contribute to these early discussions on this important topic and welcome the ability to contribute further as more detail becomes available. In the meantime, if further discussion would assist, please contact the Law Reform Adviser to the Law Society's Human Rights and Privacy Committee, Amanda Frank (amanda.frank@lawsociety.org.nz).

Nāku noa nā,

Arti Chand
Vice President

13 Ibid, at s 92.