Submission on discussion document: Options for establishing a consumer data right in New Zealand

Privacy Foundation New Zealand

Privacy in the Internet Economy working group

Summary

The Privacy Foundation of New Zealand (the Foundation) is pleased to provide its submission on Ministry of Business, Innovation and Employment's (MBIE) discussion document outlining options for establishing a consumer data right (CDR) in New Zealand. The Foundation strongly agrees with the introduction of a CDR because it will help to further protect New Zealanders' right to privacy and lay the foundation for the introduction of other essential data privacy rights in New Zealand. The Foundation assumes an equity lens has been and will continue to be applied to the development of a CDR to ensure it does not create new barriers or increase inequities.

In order to provide a holistic and comprehensive response, the Foundation's submission has been structured around the three main questions in the discussion document. In summary, our responses to the questions are as follows:

1. The Foundation strongly agrees that New Zealand needs a CDR that is framed as an individual privacy right without the inclusion of 'product data' within its focus.
2. The best form for a CDR would be to establish an economy-wide right through legislation. That legislation should ideally be compatible with the existing Privacy Act 2020 to simplify compliance, avoid gaps and duplication of activities of regulators.
3. There are a number of essential characteristics that a CDR would need from the outset in order to be effective; broad rules, an accreditation regime, a suitably equipped enforcement agency, application of the principles of Te Tiriti o Waitangi and a robust monitoring and evaluation programme.

Detailed submission

Does New Zealand need a consumer data right?

We strongly agree that New Zealand needs a CDR to support individuals' right to privacy and provide them with a clearly defined mechanism to move their data between businesses. This ability to switch between providers of a service will encourage more competition in these markets, which will inevitably reduce the price of these services for consumers. This mechanism will benefit businesses by reducing the administrative burden of transferring personal information between organisations.

The CDR comes with disadvantages, such as the cost of implementing systems and processes to meet the CDR's requirements. These costs are likely to be more burdensome for smaller businesses, so MBIE should consider initiatives that would help to mitigate this.

As for the scope of the CDR, the discussion paper frames the CDR as "foster[ing] greater consumer data portability and realis[ing] the consumer welfare and economic benefits".[1] This framing needs to be reconsidered in light of the recent amendments to the Privacy Act 2020 which aims to protect an individual's right to privacy and "giv[e] effect to international privacy obligations and standards".[2] Furthermore, the principles of Māori data sovereignty include the concepts of kaitiakitanga (guardianship) of Māori data as well as rangatiratanga (authority) over the storage, modification and exchange of Māori data.[3]

Therefore, we encourage MBIE to reframe the CDR as an ***individual privacy right***, akin to the General Data Protection Regulation's (GDPR) right to data portability.[4] It would be beneficial if our right was interoperable with data portability. That would strengthen our status of the economy providing 'adequate' protection of personal information and help our tech sector to expand their services across the borders. We also encourage MBIE to remove the 'product data' from the scope of the CDR. This aspect dilutes a CDR because it is now tasked with both improving individuals' control of their personal information and encouraging the exchange of information in a market (i.e. product data). In our view, the latter is an outcome of the former and therefore does not need to be built into the concept of a CDR.

Finally, in our view, there is still real potential to create new barriers and/or increase inequities with the CDR. That potential could be realised in the sphere of economic interest of individuals but also in the sphere of their non-economic interests. For example, personal information about the individuals can be revealed without their meaningful authorisation which would create privacy harm. Privacy, in this respect, is the ability to meaningfully control information about oneself and not merely a potential concern, as presented in benefits/cost analysis.[5] We believe that that should be identified in the current phase of development of the idea. Furthermore, suitable review processes within an effective monitoring and evaluation programme for the CDR should be implemented to identify whether any of these concerns materialise.

What form could a consumer data right take?

We believe that Option 3 is the best form for a CDR in New Zealand. This approach has a number of advantages:

- The CDR is established by legislation, which provides additional opportunities for public input through the Select Committee process and helps to clearly establish the boundaries of a CDR.
- Ensures that the CDR focuses on improving individuals' control of their personal information without the additional aspect of encouraging the exchange of product data.
- Lays the foundation for the introduction of further data privacy rights in New Zealand, similar to the data privacy rights found in the GDPR.

In our view the new right should be an extension of the existing access rights under Privacy Act 2020. That would simplify the implementation of the system and avoid the duplication of obligations and the duplication of activities of regulators.[6]

We note that the Australian approach to establishing a CDR is similar to Option 2. The Competition and Consumer Act 2010 sets out the core framework for the Australian CDR. The Australian Competition and Consumer Commission (ACCC) is responsible for issuing rules under the Act that introduces the CDR into specific sector. While this approach provides organisations with clear guidance around implementing the CDR, it is somewhat cumbersome and does not fit well with the principles-based approach in New Zealand's privacy legislation.

[1] Discussion document, p11. It is worth noting that the definition of 'consumer' (p 5) covers all actual and potential purchases and causes the CDR to be applicable also in B2B transactions.
[2] Privacy Act 2020, s 3.
[3] Te Mana Raraunga "Principles of Māori Data Sovereignty" October 2018 < www.temanararaunga.maori.nz>.
[4] General Data Protection Regulation (GDPR), Article 20.
[5] Discussion document, p10.
[6] It is worth noting that New Zealand already has such portability right in relation to health information, that is defined in s 22F of the Health Act 1956 and enforced by Privacy Commissioner.

How could a consumer data right be designed?

Assuming that Option 3 is the preferred form for the CDR, we propose that the CDR would require the following essential characteristics:

- Broad rules that outline the scope and operation of the CDR, with detailed rules set out in a regulation or a code issued by a regulatory body (e.g. the codes of practice that the Office of the Privacy Commissioner (OPC) can issue under the Privacy Act 2020).
- An accreditation regime; essential requirements that a business must meet in order to properly observe individuals' CDR. Again, detailed rules can be set out in a regulation or a code.
- Enforcement of the CDR by a regulatory body (discussed below).
- We agree with MBIE's aim to develop the CDR in a way that "builds trust and value for Māori" and in accordance with the principles of Te Tiriti o Waitangi. The design of data portability should encompass the concept of data sovereignty.
- The proposed rights should be assisted by practically meaningful processes of data management that are focused on individuals and enable them to maintain the fullest possible control over their personal information. That means that those processes should enable meaningful, informed consent that is possible to revoke any time together with the real possibility to erase personal information that has been collected about them.
- The above needs to be implemented after active consultation with 'marginalised' communities that may potentially be harmed by the improper use of personal information (especially minorities).

In our view, New Zealand's CDR should be enforced and regulated by a single government agency instead of multiple agencies to help administer the CDR more efficiently. By way of comparison, regulation and enforcement of the Australian CDR is provided by at least three government agencies:[7]

- The ACCC makes the CDR rules and monitors compliance.
- The Office of the Australian Information Commissioner (OAIC) handles complaints under the CDR scheme.
- The Data Standards Body (DSB) creates technical standards to manage the exchange of consumer data.

We believe that the OPC is the logical choice for administering the CDR, particularly given the CDR's focus on protecting individuals' data privacy. We note that this approach will require an expansion of the OPC's powers and funding to ensure that it can administer the CDR in a responsive and timely manner.

About the Privacy Foundation New Zealand

The Privacy Foundation New Zealand was established in 2016 to protect New Zealanders' privacy rights, by means of research, awareness, education, the highlighting of privacy risks in all forms of technology and practices, and through campaigning for appropriate laws and regulations. Its membership has a diverse range of professional, academic and consumer backgrounds and the Foundation regularly lends its collective expertise to comment on proposed regulation or programmes in the media or by participating in consultation processes.

[7] Australian Competition and Consumer Commission "Consumer data right (CDR)" < www.accc.gov.au>.