Submission on Discussion Document: Options for establishing a consumer data right in New Zealand

Kylie Jackson-Cox, LLB (VUW), LLM (Hons) (Auck)
PhD Candidate, Commercial Law, University of Auckland

12 October 2020

Introduction

Thank you for the opportunity to submit on the proposed consumer data right (CDR) for New Zealand. I am currently a third year PhD candidate at the University of Auckland. My thesis considers whether historical facts that are in the public domain warrant protection under privacy law. My research intersects in important ways with issues like the right to be forgotten, rights to erasure, the General Data Protection Regulation (GDPR), privacy as a human right and competing interests like freedom of expression and technology and innovation. I am happy to be contacted about any aspect of this submission.

Submission Scope

My submission is directed at the following discussion document questions:

- Does New Zealand need a consumer data right?
- What types of data should be included or excluded from a consumer data right (i.e. 'consumer data' and 'product data')?
- What form could a consumer data right take in New Zealand?
- Do you agree with the key elements of a data portability regime? Are there any elements that should be changed, added or removed?
- Do you have any suggestions for considering how Te Tiriti o Waitangi should shape the introduction of a consumer data right in New Zealand?
- Do you have any comments on where a consumer data right would best sit in legislation?

Executive Summary

1. I support the introduction of a CDR but argue that the name is inappropriate. The "right" should be renamed as "data portability", or something similar, to better reflect the tool being provided to consumers.

2. I support option three (3), and believe that it needs to be housed within the Privacy Act 2020. For data that does not meet the definition of personal information (PI) (for example, business data) then corresponding provisions could be included in the Fair Trading Act.

3. The regime needs to focus on the rights of the individual (or business), and while existing controls like consent and security are important, in light of the limits of these controls (discussed below) strengthened ancillary rights, like the inclusion of an erasure tool akin to art 17 of the GDPR, must be considered.

Detailed Submission

Does New Zealand need a consumer data right?

Yes. I believe that a CDR is a worthwhile tool for New Zealand to introduce. To the extent that strengthened consumer control over the ability to transfer data between service providers will generate increased competition in some markets, then there is potential for benefit to consumers in the long run. However, the tool must have appropriate controls, because as recognised in the discussion document, it is likely to result in a substantial increase in the amount of data transferred throughout the economy, with potential increases in risks to consumers.

However, I argue that the name – CDR – is inappropriate. Individual consumers in New Zealand have no existing data "rights". The Privacy Act does not grant any "rights" to individuals,[1] and calling this a "right" seems to be overstating its impact. What is essentially being proposed is an increased ability to control the flow of data. It seems to me that the term used in the GDPR – data portability – is more reflective of what is actually being achieved by the CDR. Utilsing that terminology or similar (data transfer perhaps) is, therefore, to be preferred.

Do you have any comments on the types of data that we propose be included or excluded from a consumer data right (i.e. 'consumer data' and 'product data')?

The decision on the type of data included in the regime appears to reflect an underlying tension in the proposed regime. The regime appears to be a potentially confusing mixture of a competition-enhancing regime (i.e. making it easier for businesses to have access to data to enter specific markets) and a consumer/data protection regime (giving individuals greater control over their data). Greater clarity might be obtained by splitting up the objectives and dealing with them separately. For example, competition law/fair trading law addresses the competition elements, with the Privacy Act housing increased protections for individuals and their personal information as a result of the competition objectives.

What form could a consumer data right take in New Zealand?

I support option three (3). I argue that sector-specific regimes introduce a level of complexity that is unnecessary. One of the arguments for the regime appears to be that data portability is happening anyway, but in an inefficient and unprotected way.[2] If this is correct, then a sector-specific approach will only ever be a lagging mitigant as technology and sectors who want to innovate will always be ahead of the regulatory response. An economy-wide approach will ensure all future developments happen safely and appropriately from the start. Furthermore, providing some consumers with rights in excess of other consumers introduces a level of complexity into our data protection regime that as a jurisdiction we have managed to avoid with a broad-brush, high level principle, approach.

I also argue that the protections need to be included in the Privacy Act (even if protections for business data need to be dealt with separately).[3] Over more than 25 years the Privacy Act has built up a reputation as the go-to place for data protections and including this important protection in a separate Act will water down the effect of the Privacy Act and potentially introduce confusion into what is generally a well-known regime. Furthermore, the Privacy Act has a ready-made process for

---

[1] Privacy Act 2020, s 31. See also Kylie Jackson-Cox "A 21st Century Right? An Analysis of the Extent to which New Zealand's Privacy Act 1993 Provides a Right to Be Forgotten" (2019) 28 NZULR 561 at 571.

[2] MBIE "Discussion Document: Options for establishing a consumer data right in New Zealand August 2020" (August 2020), paras 13 and 14.

[3] A split legislative regime covering differing types of entities is not unknown in New Zealand. For example, the Anti-Money Laundering regime is split between different legislation dependent on the particular entity.

dealing with sector-specific issues, with the existence of specific codes of practice for credit information and health information. If sector-specific or topic specific matters need addressing outside the main Act, then this process can be easily utilised.

Do you agree with the key elements of a data portability regime as outlined in this section? Are there any elements that should be changed, added or removed?

Having argued for a different design to the CDR regime, there are aspects of the proposed regime which do not apply to an economy-wide approach, for example designation. However, I believe that other aspects remain relevant, including informed consent and security and safety. However, I argue that there are other mechanisms that are required to properly deliver the outcomes this regime is trying to achieve from a consumer protection/data protection perspective. My specific points in this regard are set out below.

1. **Informed Consent:** Ensuring consumers are fully aware of the nature of the data transfer they are authorising is important. The GDPR includes a regime of "informed" consent and this could be used as a model here.[4] It should, however, be recognised that an informed consent regime is arguably stronger than the authorisation/consent regime seen in the Privacy Act. The Act has what can really only be called a "weak consent" regime.[5] The development of a more informed consent regime is something that the government might wish to pick up more broadly for the Privacy Act. This will not only ensure consistency across all data "rights", but also help to solve the issue noted below.

2. **Issues with notice and consent:** The issues with "notice and consent" regimes are well documented. The notices are legalistic, hard to find, long and mostly unread. For example, it has been estimated that if a person read all the privacy notices of all websites they used in a year it would take 244 hours. That is 10 full days, or 30 days of a usual working day (e.g. 8 hours).[6] It is, therefore, important that what makes consent "informed" is considered closely. However, the issues with notice and consent can also be addressed with other "after-the-fact" tools, which means that persons who have not read the notices or cannot understand the notices have the ability to change their minds and have their data deleted. The most common tool in this regard is the "right to erasure", as seen in art 17 of the GDPR. I strongly believe that such a tool is required in the Privacy Act to counter the risks associated with what will be the inevitable outcome of this regime – increased data being transferred and traded in the economy.

3. **Issues with IPP 9:** One of the biggest risks of increased data portability is that more organisations will be holding PI under the existing rules regarding data retention. These rules, set out in IPP 9, are notoriously ineffectual in ensuring that organisations actually delete data once its purpose has expired.[7] More organisations holding information for long periods of time increases risks around breaches and misuse. The recent introduction of breach notification will assist to manage some of these risks, but a right to erasure is also needed to ensure that consumers can have their data removed if they think the risks are too large, or if the risk of a breach materialises and they no longer wish the organisations to hold their data.

4. **Safety and security:** To ensure the safety and security of the data being transferred, an accreditation regime has been proposed. While little detail has been provided about how it is intended that this works, it appears that the third party organisations will be accredited, and therefore both consumers and the agencies holding the PI can have comfort that the

[4] General Data Protection Regulation, recital 32 and art 7.
[5] Jackson-Cox, above n 1, at 583.
[6] For example, see Ari Ezra Waldman "Privacy, Notice, and Design" (2018) 21 Stan Tech L Rev 74 at 77.
[7] Jackson-Cox, above n 1, at 575-577.

third party is trust worthy prior to data transfer. However, under the Privacy Act, any organisation that holds PI must comply with IPP 5. It must be assumed, therefore, that the particularly sensitive nature of the PI that is likely to be transferred under the CDR regime (for example, financial information) makes additional security arrangements necessary. It seems to be that this is a sensible approach, and one that should be applied more broadly across the economy. Why should other organisations that hold sensitive data not have to be accredited in a similar way? More stringent security requirements for all holders of sensitive PI would not only increase consumer confidence economy-wide, but also assist to mitigate breach-risks more generally.

Do you have any suggestions for considering how Te Tiriti o Waitangi should shape the introduction of a consumer data right in New Zealand?

It is important the Maori data sovereignty is given full consideration in this (and all PI) issues. Particular consideration of this aspect will require appropriate consultation with Maori. From literature I have reviewed, it seems to me that Maori take more of a lifecycle approach to data, which is potentially inconsistent with the one-off authorisation-for-use approach which underpins the Privacy Act. Increased touch-points back to Maori in the ongoing lifecycle of data may need to be inbuilt into the regime to ensure appropriate consistency with the government's obligations under Te Tiriti o Waitangi.

Do you have any comments on where a consumer data right would best sit in legislation?

See comments above about the strong preference for it being included in the Privacy Act.