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

10 October 2024

Communications Policy, Building, Resources and Markets Group
Ministry of Business, Innovation and Employment

By email: consumer@mbie.govt.nz and energyuse@mbie.govt.nz

Tēnā koe

Exploring a consumer data right for the banking and electricity sectors

1 Introduction

1.1 The New Zealand Law Society Te Kāhui Ture o Aotearoa (**Law Society**) welcomes the opportunity to provide feedback on two discussion documents prepared by the Ministry of Business, Innovation and Employment (**MBIE**):

(a) *Open banking regulations and standards under the Customer and Product Data Bill* (**banking discussion document)**; and

(b) *Exploring a consumer data right for the electricity sector* (**electricity discussion document**).

1.2 The following feedback from the Law Society has been prepared with input from the Society's Commercial and Business Law Committee.[1] It provides:

(a) some general comments relating to limited detail in the discussion documents and the need for more consideration of the scope of the Privacy Act;

(b) specific comments addressing aspects of the banking and electricity proposals.

2 General comments

The discussion documents are high level

2.1 Generally, the discussion documents contain limited detail about possible proposals and the pros and cons of various options. This makes it difficult to form a view on many of the specific issues on which the documents seek feedback. For instance, taking examples from the banking discussion document:

(a) The discussion document indicates that in overseas jurisdictions where consumer data right (**CDR**) regulation has occurred, those regulations have been a critical factor in determining the uptake and success of CDR. It seems to suggest

[1] More information about this committee can be found on the Law Society's website: https://www.lawsociety.org.nz/branches-sections-and-groups/law-reform-committees/commercial-li/

that in more closely regulated jurisdictions, uptake and success may have in fact been less than other jurisdictions (e.g. Singapore, Brazil). However, there is limited analysis of why this may be the case (i.e. what has led to success in some jurisdictions and not others).

(b) There is limited cost/benefit analysis which could help to understand what the benefit of the consumer data right could be relative to costs — particularly as those costs may be passed on to consumers.

(c) The discussion document mentions the Digital Identity Services Trust Framework Act. It notes that DIA and MBIE are working together to ensure alignment between the regimes. It would be useful for more information to be made available about what this looks like, and for consultation to be undertaken.

(d) Similarly, the discussion document mentions some of the work of the Commerce Commission. The Commerce Commission has a range of powers and may play a role in relation to open banking in various ways. In the Law Society's view, understanding what the Commerce Commission may or may not do in this space, and what ongoing role they could have, would assist in forming a view on the proposed regulation.

2.2 Given these points, the discussion documents may lead to broad feedback on a wide range of issues, from a wide range of parties. The Law Society would welcome further consultation once the proposals and issues canvassed in them are further advanced.

Need to further consider the Privacy Act

2.3 Privacy is a key area where necessary and appropriate safeguards, and the interface of CDR regulation with the Privacy Act, could be better considered if the proposals were more specific and developed. The Law Society is concerned to note, throughout both the banking and electricity discussion documents, multiple references to relying, for the purposes of enforcement, on provisions of the Privacy Act.[2] This approach will be inadequate.

2.4 As the Law Society outlined in its submission on the Customer and Product Data Bill,[3] the relationship between the Privacy Act and CDR needs more thought and the Privacy Act has limitations in this context. As an enforcement mechanism, the Privacy Act is too limited to address the issues that could arise, because it can only apply to personal information (defined as "information about an identifiable individual").[4] It is a framework for protecting an individual's right to privacy and right to access their information — individual being defined as a "natural person".[5] This means that, even if the Office of the Privacy Commissioner were to release an information privacy code, it would not apply to non-personal information. In the context of a consumer data right,

---

2 MBIE Discussion paper *Open banking regulations and standards under the Customer and Product Data Bill* (August 2024) (**Banking discussion document**) at paras 83, 114, 146 and 199; MBIE Discussion Paper *Exploring a consumer data right for the electricity sector* (August 2024) (**Electricity discussion document**) at paras 51–52 and 95.

3 The Law Society's submission is available on our website: see Customer-and-Product-Data-Bill.pdf (lawsociety.org.nz) and Customer-and-Product-Data-Bill-supplementary-submission.pdf (lawsociety.org.nz)

4 Privacy Act 2020, s 7.

5 Privacy Act 2020, ss 3 and 7.

consumer entities whose data is being handled will include organisations. The Privacy Act provides no recourse in this scenario. Further consideration is needed of this issue, and around the interface between the two Acts.

3 Banking

Information security

3.1 The banking discussion document sets out options in relation to information security.[6] This is an example of a situation in which the Law Society considers that it does not make sense to rely simply on the protections in the Privacy Act (Option 1). Under this approach, data that is about an organisation rather than an individual could be treated differently, and have different protections applying to it. In the Law Society's view, this could be problematic – particularly as the line regarding what is and what is not personal information can sometimes be blurry. The Law Society considers that it would make more sense for the regulations to either:

(a) include principles or specific information security requirements that apply to all CDR data (whether personal or not); or

(b) effectively deem the Privacy Act to apply to all CDR data — so that if the OPC established a code, it would apply to all CDR data in the same way (whether it is related to an individual or an organisation).

3.2 Regarding the appropriate level of prescription in setting information security standards, in the Law Society's view some certainty is needed about what will constitute reasonable safeguards. One approach could be to empower a regulatory body to provide ongoing guidance or even require certain safeguards for the data. If the choice is made not to prescribe particular standards, consideration should be given to whether the bank or the accredited provider should have to inform the customer about the differences between the security practices and protections that different providers (including unaccredited providers) might have in place compared to the bank's own systems, so that customers can give truly informed consent. Otherwise, there may be a risk that a customer could assume that a bank will only share data with entities that have a similar security profile.

Provision of customer data to unaccredited entities with consent

3.3 The banking discussion document proposes that an accredited intermediary may, with consent, make a subsequent disclosure of customer data to a different unaccredited person.[7] They may, for example, request information about the customer's transactions, and then disclose derived information such as the customer's total income and expenses (also customer data). As the discussion document explains (emphasis added):[8]

> We do not propose that unaccredited persons receiving customer data (whether designated customer data or data derived from designated customer data) be required to become accredited. *We also do not propose they be subject to any restrictions on their use and disclosure of that data other than (for personal information) complying with the*

6 Banking discussion document at para 114.
7 Banking discussion document at para 144.
8 Banking discussion document at para 146.

Privacy Act 2020. We also do not propose that accredited or unaccredited persons receiving customer data be treated as data holders.

3.4 In the Law Society's view, the rationale for enabling an accredited requestor to be acting primarily as an intermediary for a non-accredited business purely on the basis (without more) that a customer has consented is unclear. This could potentially undercut the benefit of requiring that requesters are accredited, and the criteria needed to achieve accreditation.

3.5 This is also an example of the kind of scenario in which there are likely to be problems with relying solely on the Privacy Act protections that apply to non-accredited businesses. These protections will not apply to all CDR data.

API specifications for customer data and payments

3.6 Regarding API technical standards, responsibility for the standards, and for updating them over time,[9] the Law Society recommends that there should be a regulatory body which is responsible for:

(a) setting the standards on an ongoing and evolving basis; and

(b) determining when updates must be complied with.

3.7 The body should be funded to perform these functions and to enforce requirements. The banking discussion document seems to suggest that, at least in the short term, this would be the API Centre's job, but that with time institutional arrangements might need to change. Again, this is an instance where it is hard to comment on the options without better understanding matters such as:

(a) where the expertise likely to be able to undertake the functions currently sits and how difficult it would be to build it in another organisation;

(b) what has been done in other jurisdictions and what has worked well; and

(c) what costs are likely to be involved.

Liability

3.8 The Law Society considers that a bank should have the discretion to refuse to process a payment or share data in certain circumstances (e.g. where it has grounds to suspect fraud). If there are circumstances where a bank will not have discretion and will simply have to action the request (perhaps on a largely automated basis without any real scope for due diligence), a statutory safe harbour protecting them from liability seems appropriate. This could provide that if the issue was due to the act or omission of an accredited requester, the requester should ultimately be liable. If responsibility for dealing with the customer in such circumstances and perhaps compensating them will sit with the bank in practice, there should be an ability to recoup the costs from the requester, and perhaps a mechanism or body for resolving disputes.

---

9 Banking discussion document at question 45 and section 10 (implementation, monitoring and review).

Fees

3.9 While it is likely reasonable that some fees may be charged (i.e. banks should not bear all the costs), there is also likely to be benefit in restricting these.[10] The Australian approach of making some access free while premium APIs may be charged for could be considered as one possible model.

4 Electricity

Electricity Industry Participation Code requirements: amending the Code

4.1 The electricity discussion document explains some of the deficiencies of current requirements under the Electricity Industry Participation Code 2010[11] and explains how the CDR could potentially address them. However, some electricity stakeholders have considered that electricity should not be designated until issues are learned from banking. The Electricity Authority also has an existing work programme that could address some (although potentially not all) of the present concerns and deficiencies.

4.2 These considerations may make the merits of early electricity sector designation more doubtful. In the Law Society's view, it may be preferable for the Electricity Authority and MBIE to work initially to amend the Code to address the problems, to the extent they can be achieved through Code amendments, and then assess how successful that has been before overhauling the regulatory regime for the sector more significantly.[12] This is particularly the case given that switching is already provided for under the Code. Consistent with this, the paper does not suggest that any actions should be designated. The scope of the proposal appears confined to consumer data and product data sharing.

Unaccredited third parties

4.3 Like the Customer and Product Data Bill, the electricity discussion document contemplates that third parties who are not accredited could still offer services to the consumer. Regarding these providers:

(a) It is unclear how MBIE intends to draw a distinction between service providers who would need to be accredited and those who would not.

(b) Unaccredited providers would still have obligations under the Privacy Act 2020. However, as earlier noted, the Law Society has concerns that relying on Privacy Act protections applying to third parties does not ensure sufficient safeguards and may be unworkable. Not all consumer data will be personal information subject to the Privacy Act, but could still be sensitive: for example, consumer information about a business' power consumption. There could be scope for debate about whether some information is "personal" (e.g. is an installation control point/ICP "personal information", and in what circumstances?).

---

10 Banking discussion document at question 28.

11 Electricity discussion document at section 3.

12 The Electricity discussion document notes that the Electricity Authority and MBIE are working together to avoid duplication, gaps and overlap: para 43. However, what this involves in practice is not clear.

Designating metering equipment providers as data holders?

4.4 The electricity discussion document suggests that metering equipment providers (**MEPs**), who will be data holders, will not initially be designated,[13] but that retailers will be designated.[14] Reference is made to the fact that retailers often contract out data obligations to MEPs, but it is not clear whether this is always the case, and, regardless, whether there might be some benefit in consumers or service providers being able to receive information directly from MEPs (e.g. for timeliness, or the type and format of data received).

4.5 If the intention is not to designate MEPs as data holders, it would be helpful to better understand the rationale.

5 Next steps

5.1 We would be happy to answer any questions or to further discuss this feedback. Please feel free to get in touch via the Law Society's Law Reform & Advocacy Advisor, Shelly Musgrave (shelly.musgrave@lawsociety.org.nz).

Nāku noa, nā

Jesse Savage
Vice President

13 Electricity discussion document paras 51 and 74.
14 Electricity discussion document at para 77.