Submission on discussion document: 'Unlocking value from our customer data' and on the Customer and Product Data Bill

24 July 2023

Executive Summary

The Privacy Foundation New Zealand (the Foundation) is grateful for the opportunity to contribute to the discussion paper 'Unlocking Value from Our Customer Data' and the exposure draft of the Customer and Product Data Bill (CPD Bill).

We note the limited period for which comments were sought on the CPD Bill and accompanying materials and documents. This limitation has impacted our ability to provide comments at a level that this topic warrants. We have endeavoured to provide comprehensive comments on this significant topic. However, our focus has been primarily on privacy and security considerations, rather than addressing the questions outlined in the discussion document.

The Foundation acknowledges that the CPD Bill proposes a framework that enables customers to instruct entities (such as banks) to share their information with them or with accredited requestors. We understand that the objective is to facilitate real-time product comparisons, manage accounts across various providers simultaneously, and simplify the process of switching providers for customers with an overarching goal to stimulate competition in the market. This approach has potential, as demonstrated by the successful adoption of open banking services in the UK.[1] However, we also recognise that uptake can be slow, as seen in Australia.[2]

The Foundation's feedback is categorised under the following key areas:

1. Data sharing risks
2. Consent
3. Interaction with the Privacy Act 2020
4. Enforcement
5. Strategies for maximising the uptake of the CPD system

As a fundamental consideration, we posit that privacy, trust, and customer confidence are critical to the success of the system proposed by the CPD Bill. Trust, which encourages customers to engage with other service providers, should be fostered not merely by the system's convenience, but by minimising data sharing risks, offering clear and standardised consent mechanisms, and ensuring

[1] In February 2023, the UK had 7 million open banking users (source: Statista.com)
[2] The number of users in Australia is not reported, but the review of the CDR regime notes very low awareness and uptake of the new services, see the *Statutory Review of the Consumer Data Right,* pp. 38-42.

robust and user-friendly enforcement mechanisms that safeguard customer data and protect customers from potential harm.

We observe that the discussion paper asserts that the Bill strengthens Privacy Act protections for individuals. However, the consultation documents do not appear to demonstrate effective means to support this claim. Privacy protections could be fortified if the CPD Bill conferred specific legal rights related to individuals' data or allowed the individuals to demand actions such as data erasure upon request. From our analysis of the documents, we believe the concept of a 'Consumer Data Right' no longer seems to be reflected in the CPD Bill. This may undermine customer confidence and the purpose of the CPD Bill.

1. Data sharing risks

The CPD Bill enables the transfer of personal data by means of automated electronic system (the CPD system). The mass use of the CPD system has the potential to escalate the risk of data breaches. Without sufficient guard rails built into the design of that system and services, this may reduce confidence and trust in the regulated data exchange and contribute to serious privacy breaches in the future. In this context, the CPD Bill may introduce privacy risks and undermine privacy protection without stringent controls regarding handling, security and appropriateness of data, including prevention of unauthorised or illicit access or exchange.

To promote the safety of services, and to foster trust in these services and systems, it is essential to establish explicit boundaries on data exchange both within the CPD system and beyond it.

Specifically, we note the following concerns and recommendations:

A. Handling of customer data

We propose that certain aspects of handling customer data should be enhanced in the CPD Bill:

i. **Deletion of customer data when the authorisation ends.** The Foundation suggests data no longer required for providing services (for example, after the expiration or withdrawal of consent) should be deleted or de-identified. While this requirement may be established in secondary legislation (regulations), we believe this is such a crucial to promote customer trust that it should be explicitly stated in the Bill.

ii. **De-identification.** We propose that the law should provide a clear definition of de-identification, with further regulations offering additional guidance and standards.[3] De-identification is often a source of risk for individuals due to the common misconception that removing direct personal identifiers from personal information eliminates the risk of re-identification. The standard of de-identification should be set by the regulator, taking into account the level of risk to the individuals and trust in the system. We recommend the CPD Bill is specific in its requirements for de-identification and requires transparency from agencies around the processes relating to de-identification.

iii. **Clarity on types of designated data.** The Bill defines product data as data about the product that does not include customer data. We agree with this approach, but it may be necessary to clarify that data derived or inferred from customer data are also considered customer data. Furthermore, data inferred or derived from designated

[3] More about that https://www.privacyfoundation.nz/seeing-the-forest-and-the-trees-using-de-identification-effectively-to-protect-privacy/

data should be treated the same as designated data and be subject to the same processes (e.g., deletion, de-identification).

iv. **Data security.** The discussion document indicates that security standards will outline the technical and security measures required before exchanging data. However, we note that no security measure is infallible, and data may still be stolen, lost, or exposed even when security standards are adhered to. The CPD Bill and accompanying documents do not specify which party (data holder or accredited data requestor) should respond to and manage a data breach and who is responsible for data in transit. This lack of clarity could undermine individual rights, enforcement of the Bill, the breach reporting framework under the Privacy Act, and the resolution of individual complaints.

v. Protection from unsolicited direct marketing or communications.
The Foundation recommends the CPD Bill prohibits use of data for direct marketing, similar to the Australian Consumer Data Right (CDR). Any other considerations or interactions with other regulations regarding marketing or unsolicited communications should be addressed.

B. Sharing data with third parties

Customers should be assured about the boundaries of data sharing, as this is a critical risk factor that could diminish their trust. The Foundation proposes that the CPD scheme should provide greater clarity on the responsibility for data sharing outside of the CPD scheme:

i. **Data sharing with 'secondary users'** (Section 22 of the CPD Bill): Given that secondary users can have unlimited access to designated data, we believe the CPD Bill should more precisely define this category of users. For instance, it could specify that these are users on the customer's side, such as joint account holders or staff members of business customers, as outlined in the discussion document. Moreover, Section 22 should ensure that customer data will not be shared without their knowledge or consent.

ii. **'Outsourced providers'** (Sections 23, 24 of the CPD Bill): The Foundation suggests that the Bill should explicitly state that outsourced providers, when acting on behalf of the data holder or accredited requestor, are not permitted to use designated data for their own purposes. This is a standard provision in data privacy laws worldwide. For instance, Section 11 of the Privacy Act 2020 allows outsourcing companies to avoid being treated as agencies under the Act, provided they do not use or disclose personal information for their own purposes. Similarly, the 'processor' category in the European General Data Protection Regulation (GDPR) permits the processing of personal data solely 'on behalf of the controller'.

iii. **Liability for transferring designated data outside the CPD system:** The Foundation asserts that the CPD Bill should clearly assign liability, and we deem the provisions of Section 24(3) to be essential.

C. Transborder data transfers.

We understand that the CPD Bill is intended to have extraterritorial application (Section 11 of the Bill). We note that these provisions may need to be adjusted to align with the language of the CPD Bill.[4] However, the extraterritorial scope of the law does not necessarily extend to data transfers, i.e., when an entity under the Act transfers designated data to a third party outside of New Zealand's jurisdiction (for instance, to a requestor or 'outsourced provider' from a country that does not have data privacy laws). This is addressed by IPP12 in the Privacy

[4] There is no definition of "agency" in the CPD Bill and it incorporates the broad definition of agency from Privacy Act 2020 putting under its scope, for example, government data.

Act 2020, and we are uncertain whether and how this crucial aspect for customers has been taken into account.

2. Consent

The CPD Bill positions customer consent as the cornerstone from which all CPD obligations emanate. The Foundation agrees that a clear, practical consent regime that places the customer at the centre of all decisions is essential for a CPD scheme. However, agencies and consumers may be confused by the discrepancy between the existing Privacy legislation (Privacy Act 2020) and the consent requirements in the CPD Bill. It is unclear how these requirements interact. We advise caution that the consent mechanism cannot be overly complicated and needs to be complemented with effective transparency requirements to promote informed consumer choices.

Specifically, we note the following concerns and recommendations:

A. **Consent in Privacy Act 2020.** The concept of consent in the Privacy Act does not typically serve as an authorisation for data collection/transmission, making it incompatible with the CPD Bill. This discrepancy creates confusion and enforcement issues in the event of consent withdrawal under the CPD Bill. Actions of accredited requestors and other data users against the customer's consent may not be adequately enforced under the Privacy Act 2020. For example, there will be no enforcement (i.e., no breach of IPP) if designated data is not deleted after the customer withdraws consent. The optimal solution would be to elevate the Privacy Act 2020 to global standards of consent. If this is not feasible or required, the CPD Bill should establish a specific enforcement regime around consent, which is currently absent in the Bill.

B. **Duration of consent.** To our knowledge, consumers in Australia can select consent periods, such as 3, 6, or 12 months. We believe this is a good approach. If the CPD Bill were to consider longer authorisation periods, customers would need to be reminded about the 'ongoing consent'. Alternatively, there should be a prior notification about the expiration of consent before service disconnection (e.g., 7 days in advance). This would allow customers to extend the services without interruption.

C. **Requirements for consent.** The CPD Bill (Section 30) stipulates that consent ('authorisation') must be express, including by specifying any limits on the scope of the authorisation, and reasonably informed. The Foundation suggests that detailed guidance should be issued to ensure a clear understanding of what 'reasonably informed' entails, such as the level of information required to make such consent informed.

D. **Standardising consent and customer's choice.** We also see a lot of additional value in standardising consent and the typical terms and conditions of services to which the customer consents (use scenarios). The risk is that an excess of consent requests could lead to confusion, desensitisation of customers, and potential mistrust in the system. In essence, customers tend not to read consent requests, so the structure of choice they are presented with should be as clear, structured, predictable, and non-misleading as possible.

E. **Consent 'dashboard'.** The regulation is unclear about who provides the customer with the consent option – the data holder or the accredited requestor (or both of them).

3. Interaction with the Privacy Act 2020

We observe that the proposed CPD Bill does not confer any legal rights on individuals – it provides no additional entitlements to their data, but instead imposes obligations on other users of the CPD system. We believe this is not only a missed opportunity to establish a modern, privacy-protective consumer data rights system in New Zealand, but also potential problems with clear communication of the benefits (no "consumer rights"), fostering trust in the new products, and enforcing the CPD system rules. An example of such a problem is the lack of enforcement of the use of consent for authorising data collection in the Privacy Act 2020, as described in the previous section. Without clearly defined privacy rights, it may be challenging for individuals to feel they have control over their data, when, for example, they cannot request its deletion to mitigate their risks or even to stop unwanted marketing calls.

We also note that the discussion paper states that the Privacy Act 2020 will continue to apply to data holders, accredited requestors, and outsourced providers. Therefore, all personal information remains subject to the requirements of the Privacy Act 2020, except where the draft law indicates otherwise. Regarding the interaction between the CPD Bill and the Privacy Act 2020, we note the following:

A. **"Personal information" vs "customer data".** The Foundation believes that the relationship between these two definitions needs to be clarified. Specifically, regarding the following points:
   i. **Non intuitive application of Privacy Act 2020 to some customer data**
   The Privacy Act cannot apply to those customer data that are not "personal information" (e.g., Sections 45, 47, 48). This implies that data of business customers that are not personal information remain outside the enforcement mechanisms of the Privacy Act. However, it may also be that customer data includes personal information of someone else (customers, staff, etc.). In such case, the application of the Privacy Act may be much more complicated.
   ii. **Identifiability**. The definition of personal information in the Privacy Act 2020 relies on the concept of an individual's identifiability. What makes a person identifiable may be significantly different from what makes a business customer identifiable. In particular, personal information that is stripped of direct identifiers still *remains* personal information (because there are other ways of identifying an individual and potentially harming that person), while information about business customers could differ in this respect. Also, the principles and rights behind protecting personal information and business information are different (e.g., privacy vs trade secrets/confidentiality).
   iii. **"Information" vs "data"**. Finally, the Foundation believes that the Bill should clarify what is understood as information and what is understood as data, to address the different use of terminology. There are different theories and varying practical understandings regarding both terms and clarity is necessary to avoid confusion regarding scope and intent. For example, some believe data is information that has been recorded in digital form. Others may believe them to be the same or that data is objective, and information may be objective or subjective.

B. **"Customer data" vs "product data".** The Foundation suggests distinguishing between these two types of data may be challenging. Assuming that the concept of identifiability from the Privacy Act 2020 applies to the CPD Bill in the same way (see also above), there is minimal, if any, room for product data in the case of individual customers. This is because information about a product that an individual customer is using also constitutes information about that person. This broad interpretation of personal information under the Privacy Act has been

confirmed in case law and the practice of the Privacy Commissioner.[5] Therefore, any product data exchanged in the context of an individual customer also qualifies as customer data.

C. Interaction with IPP6 of the Privacy Act 2020.

i. Section 46 of the CPD Bill stipulates that several provisions of the Privacy Act 2020 do not apply to the CPD request (for instance, provisions relating to urgency, assistance). We suggest that the selection of sections for which the Privacy Act 2020 do not apply be revisited. We recommend it should include Sections 50, 52, and 54 of the Privacy Act 2020. That is because customer data is not likely to contain any evaluative material; trade secrets should not be a reason to reject an authorised request in a regulated CPD system (it could be argued that all customer data is a trade secret); and data holders should not impose further conditions on releasing the designated data.

ii. The interplay between the CPD Bill and the Privacy Act 2020 may create confusion, as it establishes a two-tier system for handling access requests. Given the imperfect enforcement mechanism of the Privacy Act 2020 (more on that below), the Foundation's view is that the procedure for exchanging customer data should be as simple and straightforward as possible, enabling the Privacy Commissioner to create a fast-track for investigations related to customer data.

D. Resources for enforcement of Privacy Act 2020.

In the Foundation's view, it is highly likely that the increased data exchange will lead to a rise in the number of complaints and notifiable privacy breaches under the Privacy Act 2020, especially if customers are confused or misled. It would be necessary to ensure the Office of the Privacy Commissioner is sufficiently resourced to handle this increased number of complaints.

4. Enforcement of the CPD Bill

The Foundation observes that aside from the enforcement of some elements of the CPD Bill through the Privacy Act 2020, there is little mention of the enforcement of the CPD Bill.

The Privacy Act 2020 cannot provide adequate enforcement schemes if the customer data is not personal information and for actions which extend beyond the processing (that is, collection, use, and disclosure) of customer data. However, action initiation (Sections 17-18 of the CPD Bill) in relation to individual customers will inherently involve some use or disclosure of personal information, and privacy complaints may arise from it. Therefore, the CPD Bill should also clarify that it does not prevent privacy claims in relation to all other actions in a similar way as it does for storage and security requirements in Section 48.

Also, the Privacy Act 2020, by the nature of its enforcement regime, is not equipped to enforce obligations related to real-time data exchanges. The complaints initiate investigations are focused on achieving settlement and often last longer than a few days.[6] If the government plans to rely on this enforcement system, the privacy enforcement regime might need an overhaul and strengthening.

---

[5] E.g. Case Note 228045 [2012] NZ PrivCmr 8, Advisory Opinion AO 1/2016 [2017] NZPrivCmr 1, *Taylor v Corrections* [2018] NZHRRT 35.

[6] E.g. in 2022 33% of closed complaints last longer than 6 months (PC annual report for 2022).

The future enforcement scheme, which will be set out in Part 4 Subpart 3 of the Bill, should provide for quick procedures enabling customers to resolve disputes and receive appropriate redress from those parties to the CPD scheme in case of contravention or problems with switching. The authors of the Bill should be mindful of the problem of enforcement gaps if they rely on the Privacy Act 2020. The enforcement scheme should create powers for the enforcement agency to collect, share, or view personal data. Also, the Government should be prepared to bear the cost of the enforcement agency.

5. Strategies for maximising the uptake of the CPD system

The Foundation suggests recommendations and insights that we believe could be relevant for scaling a system in New Zealand:

A. Enhancing competition among current data holders. A CPD-backed system should facilitate switching between existing data holders in both directions. This provides opportunity to stimulate more intense competition among current market incumbents who could be designated as both data holders and accredited requestors. The existing market players may have access to necessary know-how and capital to change the existing market much quicker.

B. Reciprocity. The CPD Bill should allow for a win-back mechanism, enabling two-way switching of services. The data of customers who have migrated their services to new service providers should also be available for exchange. This could be triggered when a certain threshold in customer numbers or market share is reached by the new service provider.

C. Accreditation system. The proposed accreditation system and the agency system to support it will need to be of the highest standard of rigour and professionalism. This should include:

i. **Adequate insurance.** The discussion document provides a vague description of accreditation requirements, mentioning a 'fit and proper person' with adequate business insurance expertise. The Foundation believes additional measures should be implemented for confidence in the CPD system. The CPD scheme's accredited requestors, or the scheme itself, should offer some form of "safety net" for customers. This could take the form of insurance that guarantees quick reimbursement of costs (similar to the case of unauthorised credit card use) or a statutory compensation mechanism. Noting in Australia's deployment of the CDR, we recommend against safeguards that could impose unnecessary costs and barriers to new entrants, such as frequent auditing.

ii. **Cultural capability of accredited requestors.** We endorse the approach where cultural capability is not a prerequisite for being included in the accreditation regime. We believe foreign companies entering the market might face challenges in meeting additional cultural obligations, which could deter uptake of the system. Additionally, from the customer's perspective, customers may also come from diverse cultures and the system should not impose any general rules that could be perceived as limiting for certain customer groups based on their diverse cultures. We support the notion that cultural capability should serve as a differentiating factor in the market.

D. Transparency of product data. The Foundation emphasises and reiterates the importance, and need for, full transparency and availability of product data to increase competition. This is because it allows for the comparison of market offers. To ensure the availability of product data, standardisation of product parameter descriptions might be necessary. This would allow customers and accredited requestors to compare them, even when direct comparison of retail offers is not possible due to, for example, the structure of additional fees.

E. **Addressing digital competence.** The Foundation acknowledges that the requirement for digital competency from organisations holding customer data may pose challenges for many individuals and small and medium-sized enterprises (SMEs) in New Zealand. This requirement could add complexity for customers. Therefore, the Foundation suggests that policy measures around the implementation of CPD legislation and open banking (as the first application of those) should include provisions for customer and consumer education.

F. **Clear use case scenarios.** To maximise uptake, the Foundation suggests secondary regulation (e.g., for open banking) should clearly define services (use scenarios) for customers. Examples of such use scenarios include: "joint accounts" / account management service, loan assessment, comparison services, and payment service. These scenarios should be used to communicate the advantages of the regulation to customers. For instance, during difficult economic times, customers (and consumers) could be interested in comparison services that find the best market offers for their specific type of use of the service.

G. **CPD system should not hold monopoly**. We recommend the CPD-based system of data exchange should not be the sole method of data transfer between data holders and accredited requestors. There are numerous reasons why market participants may prefer to exchange data through alternative systems, and such options should remain viable. These reasons can range from greater security in cooperative services, avoiding monopolistic practices, fostering innovation in data exchange, or facilitating alternative forms of cooperation that might be influenced by cultural or ethical factors, such as data cooperatives.

6. Other remarks

A. **“Customer” vs “consumer”.** While the Bill clearly operates with the term "customer" and "customer data" (for example, as seen in section 8 of the Bill), the discussion paper creates some confusion between "consumer" and "customer". This distinction should be clarified in further communication and documents.

B. **Avoiding problems with switching.** We believe that the CPD Bill and subsequent regulations should remain flexible and allow for certain exceptions where data holders may not comply with a request (e.g., if the requests appear to be potential fraud and could clearly cause harm to the customer). We believe that data holders should be responsible for a basic level of fraud prevention.

Thank you for the opportunity to submit on this proposal. We acknowledge that this consultation had a short window of time to prepare and accept comments, and that detailed material was provided for comment. As a Foundation, we draw on our members varying expertise and perspectives to provide informed comments. This short period of time has impacted the breadth and depth of comments we were able to provide in this submission. We see tremendous opportunity with this initiative, as well as material impacts to privacy rights if not addressed carefully and would welcome the opportunity to further review and comment.

This submission was prepared on behalf of the Privacy Foundation New Zealand by Marcin Betkier, Keith Norris and Polly Ralph.

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.

Ngā mihi nui,

Dr Marcin Betkier

24 July 2023