5th September 2024

Privacy Foundation New Zealand

Submission on Customer and Product Data Bill

The Privacy Foundation New Zealand (the Foundation) is grateful for the opportunity to make a submission on the Customer and Product Data Bill (Bill).

The Foundation's submission is divided below into the following key areas:

1. General comments: privacy, trust and customer confidence are essential
2. Over-reliance on secondary regulations
3. Interaction with the Privacy Act 2020
4. Authorisation
5. Other remarks

1. General comments: privacy, trust and customer confidence are essential

The Bill proposes an economy-wide framework that aims to enable greater access to, and sharing of, customer and product data between businesses. The purposes of the Bill include facilitating competition, enabling innovation and supporting secure, standardised, and efficient data services. It will gradually be rolled out to specific wholesale markets (e.g., in banking, electricity, telecommunications) which will form the backbone of the services offered on the retail market to the customers by accredited requestors.

Importantly, the Bill also aims to enhance privacy by giving customers greater control over how their data is accessed and used. It does this by creating a set of requirements for data requests and authorisation.

We support these goals, and we support many of the proposed measures in the Bill. Having said that, we also recognise that success is likely to depend on many individual factors operating together, each of which may have an effect on privacy:

- **content of regulations which are still to be drafted:** that is, the secondary regulations setting up the wholesale regulated markets in each sector;
- **technological factors:** the market's ability to establish safe, accessible and effective systems that promote rather than undermine privacy, including:

    - electronic systems enabling customers to make requests;
    - interfaces between data holders and accredited requestors;
- **operational factors:** effective business processes that enable customer and product data requests to be made and dealt with promptly; valid authorisation processes and communications; and overall successful customer support;
- **availability of competitors that provides real choice for customers:** the availability of accredited requestors with retail services that are able to attract a broader group of customers on the retail markets and stimulate competition by allowing 'multi-homing' of services or/and easy switching between providers; and
- **promoting well-founded trust:** a large number of customers need to trust both the accredited requestors and the overall design of the wholesale market, and that trust needs to be well placed.

It is clear from the successful adoption of open banking services in the UK and some European countries that the Bill has the potential to benefit consumers. However, some jurisdictions have experienced challenges that reduce or delay delivery of that benefit. For example, we understand that in Australia the success of similar services was limited due to long implementation, low number of the Australian equivalents of accredited requestors and little customer uptake.

The central importance of customer confidence to the success of the Bill's objectives mean that it is essential that the scheme has **privacy and trust** built into every aspect of its design. That trust, which encourages customers to engage with accredited requestors and with the whole system, should be fostered not merely by the system's convenience and reliability, but by ensuring that privacy is one of the main considerations. Key factors that have informed our comments in this submission are the need to:

- minimise data sharing risks;
- offer clear and standardised consent mechanisms; and
- ensure responsible handling of customers' data and robust and user-friendly enforcement mechanisms that safeguard customer data and protect customers from potential harms. Those harms include not only financial loss or identity theft, but also damage to dignity and/or autonomy of customers (e.g., exposure of confidential transaction or telecommunication data).

We recommend that there are some relatively easy changes that can be made to the Bill to facilitate sustainable and trustworthy business models.

Ideally the Bill would confer specific legal rights related to individuals' data on them, that is, **create a true Consumer Data Right**. That change would have not only legal consequences, but also a huge impact on the public perception of the future Act.

Even without creating a broad consumer data right, however, the Bill would be improved if the following changes were made:

- **Right to deletion/erasure.** Data portability is only one part of the equation. The business from whom the information was requested may still hold that information,

often for long periods of time. If there is no specific legal reason for them to continue to hold the information (e.g., to meet other regulatory requirements or for the purposes of legal action), the Bill should permit individuals to demand that the data be deleted. That should also extend to deleting information from accredited requestors if the customer withdraws their authorisation. Knowing that their data could be deleted on request, the customers might be more willing to try the new services from alternative providers.

- **Right to limit use:** Once shared, there appear to be few limitations on what third party recipients can use the information for. This creates some significant privacy risks, which would only partly be addressed by the new transparency requirements in the Privacy Amendment Bill 2023. To the extent that the information is personal information, we therefore recommend that the Bill should prohibit secondary uses of personal information by those recipients, unless the customer expressly authorises those secondary uses. This change would usefully create an equivalent of the California Consumer Privacy Act's right to opt-out of sale or sharing of personal information.[1]
- **Right to object to personal marketing**: Customer willingness to shop around for services offered by various accredited providers could be fortified if the Bill introduced an additional protection against using customer data for unsolicited marketing. We think that would ensure customers that sharing their data will not increase the risks of receiving unwanted targeted marketing (or scams) in the future.
- **Right to non- discrimination:** It is important to ensure that the Bill protects those who choose to exercise a customer data right against retaliatory action for exercising that right (such as denial of future service, or provision of services on less favourable terms).[2] Fear of retaliatory action could swiftly operate as a brake on customers' willingness to take advantage of the new system, undermining not only the potential benefits that customers are intended to receive, but undermining the success of the system as a whole.

2. Over-reliance on secondary regulations

We noted that there are many areas that still require further development by regulations and standards. It is common to delegate technical elements to secondary legislation, but the Bill appears to go a lot further. Many crucial elements of the regulatory regime are not clear in the Bill itself and are not even guaranteed to be made publicly available before enacting those secondary regulations (clause 99 does not envisage public consultation of the designation regulations). It is possible that the content of those regulations could have a negative impact on privacy.

The unusual scope of the legislative delegation is seen particularly vividly in s 126(1)(b):

---

1 More about California Consumer Privacy Act – https://oag.ca.gov/privacy/ccpa.

2 Also in California Consumer Privacy Act.

(1) The Governor-General may, by Order in Council, on the recommendation of the Minister, make regulations for all or any of the following purposes:

(...) (b) prescribing, for the purposes of any provision of this Act that requires a thing to be done in a manner prescribed by the regulations, the manner in which the thing must be done, including prescribing—

(i) by whom, when, where, and how the thing must be done:

(ii) the form that must be used in connection with doing the thing:

(iii) what information or other evidence or documents must be provided in connection with the thing:

(iv) requirements with which information, evidence, or documents that are provided in connection with the thing must comply:

We submit that all core conditions of the framework (including core privacy protections) should sit in the primary legislation, leaving secondary regulations to provide greater detail about how to those requirements must operate in practice. Failure to do so would leave too much to broad and unconsulted administrative discretion.

Having this in mind, and understanding that perfect clarity is not possible when setting up a framework that could be used for many sectors, we also consider that the Bill should be clearer about the following points:

- **The actions relating to a customer/accredited requestor (see clauses 18 and 19)**
  Those actions are described in the Bill in very generic terms allowing too much leeway for the secondary regulation. The data holder will be forced to perform almost **any** action designated by the regulator.
  For example, under clauses 18 and 19 data holders have to perform certain actions relating to a customer/accredited requesters if the data holder would "ordinarily perform the action to which the request relates". When considering whether a data holder would ordinarily perform an action, regard must be had to the matters (if any) prescribed in regulations or standards. In the absence of regulations or standards, there seems to be a lot of ambiguity about what this may mean.
- **Joint customers (see clause 21)**
  Similarly, when dealing with joint customers/accounts under clause 21, we submit that too much ambiguity has been left to be clarified by standards. Clause 21 does not define any directions about how the regulations should resolve the issue of competing privacy interests of joint customers. This is likely to be a challenging issue.[3] For example, according to clause 21, it might be possible that the regulation will allow the personal information of one of the joint customers to be transferred to a third party without that person's knowledge or authorisation as long as it has been authorised by the other joint customer.
- **Secondary users (clause 24)**

[3] See also the question of interaction with Privacy Act 2020 below.

The Bill allows the regulations to almost freely define secondary users and we suggest that this this gives the Minister too much leeway in this privacy-critical area. Clause 24(4) explains only that a person is a secondary user when they are specified, or belong to a class specified, in designation regulations as a secondary user in relation to a class of customers, and a customer belongs to that class. Each following condition depends on the designation regulations. But that leaves the reader unsure as to who the secondary users could be and what would be the consequences if the designation regulations are described in more general terms. It creates the possibility for broad **secondary circulation of customer data** which, if not properly controlled, could damage the trust in the whole system.

- **Territorial applicability (clause 11 in relation with clauses 8(3) and 9(3))**
  The secondary regulation also attempts to define the territorial applicability of the Bill. That is because clause 11(1) of the Bill states that the Act applies to a New Zealand or overseas agency in relation to any conduct by that agency in respect of designated customer data or designated product data. However, designated customer data and product data according to clauses 8(3) and 9(3) need to be defined in the designation regulations. We submit that territorial applicability is a fundamental feature of all New Zealand law that should be included in the principal Act. While there are no doubts some sectors in which overseas businesses will feature more prominently, it is not appropriate for territorial application to be left to secondary regulations. Further, limiting applicability of the Bill to actions in relation to designated data may leave many actions that are not focused on designate data, for example, applications for accreditation not covered by the law.

3. Interaction with the Privacy Act 2020

We submit that the interaction between Bill and Privacy Act 2020 requires more attention as the existing provisions of clauses 52 and 53 leave too much uncertainty.

Clause 52 of the Bill removes the applicability of IPP6 in relation to data requests defined in clauses 14, 15, but treats any breach of clauses 14, 15, and 16(2) as an interference with privacy under Privacy Act 2020. To the extent that the information is personal information about the requester, this usefully triggers the normal investigative powers of the Privacy Commissioner, and provides customers with full access to remedies under the Privacy Act.

In addition to that, clause 53 extends the applicability of the Privacy Act's IPP5 to certain breaches of the storage and security obligations set out in the Bill. This is also a useful privacy protection.

However, outside of these two sections containing specific exceptions and extensions, the Privacy Act 2020 still seemingly applies to the remaining of the actions involving personal information under the Bill. That creates some tensions in the following areas:

- Section 24 of the Privacy Act 2020 provides that only statutory regulation can limit IPP 6, 11 and 12, but that any New Zealand law (which includes law in secondary regulations) may limit or affect other privacy principles (IPPs 1 to 5, 7 to 10, and 13) if it requires or authorises certain action taken by an agency. So, the extent to which the Privacy Act 2020 will apply depends very much on the contents of the secondary regulations which may change or lift the Privacy Act protections. Also, it is worth noting that secondary regulations cannot impact privacy protections on disclosures (IPP11) and requirements for disclosure of personal information overseas (IPP12).
- The Privacy Act 2020 applies only to personal information about individuals and does not protect customers who are not individuals (such as companies). That means that customers other than individuals will have to use the enforcement mechanisms proposed by the Bill. They will not be assisted by clause 53 of the Bill and IPP5 of the Privacy Act 2020: effective enforcement will need to come from elsewhere. Similarly, the provisions of the Privacy Act 2020 relating to notifiable privacy breaches (sections 112-122) do not apply to customers that are not individuals. Those are important protection mechanisms enforcing security that, we submit, should be extended to all customers affected by the scheme in the Bill.
- It is unclear how the provisions will affect situations involving joint customers, for instance a small group of individuals such as a group of tenants with a common bank account, electricity account, or internet account. The principles of the Privacy Act 2020 are better suited to questions about individual information rather than information about groups. For example, IPP11 (which cannot be derogated by secondary regulations) does not contain any exceptions related to disclosure of the data of one of joint customers as a result of authorisation given by other joint customer(s). That, in relation to section 24(1) of the Privacy Act creates uncertainty whether secondary regulation should define the rules for joint customers (clause 21 of the Bill). We believe that those rules should be covered by the statutory law.
- The definition of customer data in clause 8(2) of the Bill relies on the concept of identifiability of a customer (a standard privacy setting). But, when the customer is a legal person it can create additional problems, as the customer data could be an information about the customer and the information about individuals (e.g., customer employees or clients). For example:
    - In specific instances individuals could be identifiable in many customer accounts, for example as an individual customer and clients or employees of another customer.
    - The existence of personal information in the customer data of legal persons also may create problems in responsibility for data breaches. It is not certain who will be responsible for privacy breaches related to the mishandling of personal information. Should the individuals turn directly to data holders or accredited requestors or to their service providers who are customers of those data holders or accredited requestors.

  Taking this into account, we think that using identifiability as a designator to define customer data may create problems without specifying that the data should belong to

"customer account" of particular data holder. Because identifiability does not seem to be the best designator for customer data when customer is not a natural person, we suggest including and describing company data as "account data".

- We believe that the Bill should incorporate other important elements of the Privacy Act in its own provisions. Since a data request under clause 14 or 15 of the Bill does not equate to an IPP6 request under the Privacy Act, it will not trigger the administrative protections in the Privacy Act relating to matters such as timeframes for response. Most obviously, we submit that the Bill should contain provisions relating to:
  - assistance in making a request (similar to section 42 of the Privacy Act), to support accessibility needs; and
  - charges (similar to section 66 of the Privacy Act), setting out not only what can be charged for but also that those charges must be reasonable. Unreasonable costs would act as a substantial deterrent for customers to make requests. Any specific rules about charges that apply in a particular sector could then be left to the regulations.
- The interrelationship between the Privacy Act and other legislation is an area that can cause confusion both for affected people and for businesses. We suggest that clause 17 of the Bill could be expressed more directly, to avoid potential problems. For example, it could say "Nothing in sections 14 or 15 limit an individual's rights to access information about themselves under IPP6 of the Privacy Act, or to have any decision under IPP6 reviewed by the Privacy Commissioner." We submit that this could offer individuals more certainty as to how the Privacy Act and the Bill work together.

4. Authorisation

As mentioned at the beginning, we consider that the statute should provide for more specific requirements around authorisation to assure customers that they have control over their data, particularly in the context of potentially wide information sharing. The individuals need to be sure that their data (about their money, private life, secrets, identity, etc.) are well protected and that if their choice of alternative provider turned out to be a mistake, they can withdraw the authorisation and require erasure of their data (including downstream data held by secondary users), minimising their potential harms or risks of harms.

In order to be valid, authorisation should be intentional, informed, specific, and free from controlling influence. We recommend that clause 36 should be amended to incorporate more assurance that those requirements are met to a high standard. That could include requirements to ensure that:

- authorisation is freely given;
- the request for authorisation clearly specifies the purposes for which authorisation is sought, any intended further recipients of that data, and the purposes for which data may be used under that authorisation;

- authorisation must be ‘opt-in’: that is, that a customer must expressly confirm that they wish to participate. Authorisation should not be assumed, for example as one of general the terms and conditions of a service. If a person does nothing, it should be presumed that they have not authorised the transaction. Taking this approach will also assist businesses to meet the new requirements for notifying people of information collections under the Privacy Amendment Bill, currently progressing through Parliament. If people have already been properly informed and have authorised the transaction, it will remove the notification obligations from downstream collectors of that information.

- the customer is not only reasonably informed about the matter to which the authorisation requires but also about the authorisation process. That is, that customer is informed about the period for which the authorisation is active and how to end the authorisation if they wish to do so.

As mentioned earlier, we also submit that clause 37 should:

- be extended to require the accredited requestor to erase the customer data on customer’s demand when authorisation is ended (or withdrawn), unless there is a clear lawful reason to retain that information;

- require that ending authorisation should be as easy as giving it. Taking into account the problems experienced by customers with so-called “dark patterns” - deceptive interfaces and practices of some service providers related to disincentivising customers from ending authorisation or otherwise terminating their services, it is important that this legislation provides a strong assurance that the good of the customer is the first priority.

In summary, we submit that improving protections around authorisation could provide useful assurance that customer rights are respected and would contribute to engendering trust in the CPD-enabled markets and systems.

5. Other remarks

We have some other suggestions as follows:

Consultation on proposed designation (clause 99)
Given the extensive delegation to secondary regulation, we propose that clause 99 imposes a broader obligation to consult the general public on any proposed designations. We further recommend the removal of numeral 4, which currently states that a failure to comply with clause 99 does not affect the validity of the designation legislation. In our view, numeral 4 raises concerns because it suggests that any failure to properly consult on ‘designation regulations’ according to 99 is acceptable.

Testing of the electronic system
We submit that the requirements to test the electronic system on request from Chief Executive (clause 29 of the Bill) should be extended to require periodic testing. That

could be done either by extending clause 29 or allowing the regulations and standards to cover also requirements for testing (clause 28(2)).
Testing assists organisations in quickly identifying any deficiencies that may be present in their procedures and systems. Periodic testing allows quick remedial actions and ensure systems are fit for purpose and working correctly. Furthermore, it avoids surprises and provides consistency in a service which requires interoperability with other service providers in the same ecosystems. This is beneficial for data holders' cost-efficiencies procedures, regulatory bodies' enforcement and individual outcomes.

Requirements on overseas agencies
The Bill is silent as to the requirements on overseas agencies that may apply to be covered by the accreditation regime. It is likely that some market players from other countries could wish to extend their services to New Zealand, especially if those services are available globally (e.g., as Internet services or mobile apps). While not a problem in themselves, such arrangements might require some specific provisions in regulations, for example in relation to insurance or transborder data transfers (for example assurances about onward transfers of information). While the businesses would be subject to New Zealand law, including the Privacy Act, those additional requirements could provide certainty both for the service providers and for the customers.

Derived Data
Derived data, as defined in clause 33(3), is "data that is wholly or partly derived from — (a) designated customer data; or (b) other derived data." As technologies advance there is increasing opportunity for creating derived data by linking data from various contexts together to make inferences and decisions about individuals. It is often extracted or extrapolated from existing customer data in combination with other data (that may include opinions, inferences and other information that may be true or not). It may include information that is unknown to the customer, information that customer would not have chosen to reveal about themselves (e.g., an opinion that is not true), or the information organisations use to designate and facilitate the delivery of products and services to the customer.
Derived data, if it is about individual, is a personal information and can have as much value or effect as customer data. It can also create harm, for example by giving opportunity for discrimination, bias etc. Its separate definition in clause 33 and distinguishing it from designated customer data suggest that it may not be included in designated customer data. That, in turn, means lost opportunity to bring value to customers and loss of their control over their personal information.
We submit that derived data should be included in the provisions of the Bill. That is, it could be possible to request under clauses 14 and 15 and also deleted on request.

We hope that all these comments are useful for the Committee as it considers the Bill.

About the Privacy Foundation

The Privacy Foundation New Zealand Inc 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.

This submission was prepared on behalf of the Privacy Foundation New Zealand by Dr Marcin Betkier, Maria Tenorio, Katrine Evans, Annette Mills and Alexandra Chapman.

Ngā mihi nui,

Katrine Evans
Chair, Privacy Foundation New Zealand