Privacy Commissioner
Te Mana Mātāpono Matatapu

Privacy Commissioner's submission to the Economic Development, Science and Innovation Committee on the Customer and Product Data Bill (44-1)

1. I am pleased to provide a submission to the Economic Development, Science and Innovation Committee (the Committee) on the Customer and Product Data Bill (the Bill).

2. The Privacy Act 2020 is New Zealand's main privacy statute. One of the Privacy Commissioner's functions under the Privacy Act is to examine proposed legislation that may affect the privacy of individuals.

3. In the case of this Bill, I am submitting not only as part of my general function of commenting on the privacy implications of proposed legislation, but also because my Office will play an important role as the privacy regulator under the Bill.

4. The Bill would establish a consumer data right (CDR), which is a framework to enable greater access to and sharing of customer and product data between businesses. A CDR would be a positive and potentially privacy-enhancing development, so long as privacy safeguards are built in to the framework and can be properly enforced.

Executive summary

5. I support the creation of a CDR for New Zealand because it will enhance customers' control over their information. I believe the Bill would establish a CDR that is broadly appropriate for the New Zealand context and that builds in privacy safeguards. Effective protection of privacy will be essential to ensuring public trust in the sharing of personal information under the Bill, and therefore to the success of a CDR.

6. The Bill is designed to align with and be complementary to the Privacy Act. Under the Bill, the Privacy Commissioner will be the CDR privacy regulator, and this role will include functions of investigating complaints and taking compliance action in relation to CDR-related privacy breaches.

7. The Bill includes safeguards to protect the privacy and security of personal information. These safeguards include a requirement for customers to provide express and informed consent before information can be requested or actions can be initiated on their behalf. I am broadly satisfied with these safeguards, but my Office will need to be adequately resourced and empowered to ensure compliance with them. I also note that details of the safeguards will be further developed through regulations and standards.

8. As the CDR privacy regulator, my Office will play a key role in promoting public trust in and understanding of the protections for personal information under the Bill. Although these matters are largely outside the scope of the Bill, I therefore highlight the need for my Office to be resourced to effectively carry out my functions under a CDR through a mixture of levy and Crown funding; and for amendments to the Privacy Act to strengthen the Privacy Commissioner's enforcement powers.

9. I also recommend amendments to the Bill to provide more clearly for customers' control over their information to be a purpose of the Bill; to set out matters (including privacy) that must be considered in making regulations and standards under the Bill; and to require the CDR regime to be reviewed within three years of its creation.

A consumer data right would enhance people's control over their information

10. The case for establishing a CDR often focuses on benefits for competition and innovation. More fundamentally, however, a CDR would give customers more control over their own information and provide an important extension of existing privacy rights.

11. The right of individuals to access information about themselves is fundamental to legislative protection of privacy in New Zealand and other comparable jurisdictions. A CDR will help ensure that existing rights of access to personal information remain meaningful in the digital environment, by facilitating the secure sharing of customer information with the customer's knowledge and authorisation.

12. Because customers' control over their own information is so fundamental to a CDR, I recommend that the Bill's purpose clause (clause 3) is amended to reflect this. Currently clause 3(1) states that the purposes of the Bill are to realise the value of data, promote competition and innovation, and facilitate secure, standardised and efficient data services. Clause 3(2)(a) provides that those purposes are to be achieved by 'improving the ability of customers, and third parties they authorise, to access and use the data held about them by participants in those sectors'.

13. I **recommend** that clause 3(2)(a), or similar wording, be moved into clause 3(1) to become a purpose of the Bill, rather than a means by which the purposes are achieved. I further **recommend** that clause 3(1) refer more clearly to providing access to data in a way that is safe and secure. This change would be consistent with the general policy statement, which highlights the Bill's role in giving customers control over their data.

14. The Committee may wish to consider the equivalent section of Australia's Competition and Consumer Act 2010 (CCA), which provides that an objective of the part of that Act establishing a CDR is:

> to enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed safely, efficiently and conveniently:
>
> (i) to themselves for use as they see fit; or
>
> (ii) to accredited persons for use subject to privacy safeguards.[1]

The Bill establishes important protections for personal information

Privacy is central to the success of a CDR

15. While a CDR would help give effect to individuals' privacy right of access to their own information, legislation that facilitates the sharing of personal information must also include safeguards against privacy risks. Such safeguards are fundamental to gaining consumer trust in the CDR framework and ensuring customer uptake of the opportunities a CDR would create.

16. In Australia, a 2022 statutory review of the CDR found that:

> The strong privacy requirements of the scheme have supported the establishment of the CDR. They create a foundation of trust, safety and security, all of which will be central to engagement and uptake of the CDR from consumers and participants –

[1] Competition and Consumer Act 2010 (Cth), s 56AA(a).

particularly when compared to other, less secure data sharing mechanisms like screen scraping. …

[M]ost participants agree that the existing high levels of information and data security are necessary to underpin trust and confidence in the CDR, and provide a secure foundation for future expansion. For the same reasons, the privacy safeguards continue to be viewed as an important element of the CDR, especially in building a trusted system.[2]

The Bill is designed to integrate with the Privacy Act

17. One criticism of Australia's CDR is that the interaction between CDR privacy safeguards and Australia's Privacy Act is too complex. New Zealand has an opportunity to learn from this critique, and my Office has been working with officials from the Ministry of Business, Innovation and Employment to do so over the course of the Bill's development. I am satisfied that overall there is appropriate alignment and complementarity between the Bill and the Privacy Act.

18. The Bill preserves the role of the Privacy Commissioner as New Zealand's privacy regulator, including in relation to a CDR. The Privacy Commissioner will exercise the Commissioner's existing functions under the Privacy Act in relation to the handling of personal information under a CDR. These functions include investigating complaints of breaches of the Privacy Act, undertaking compliance action and receiving notifications of privacy breaches. In addition, the Commissioner will take on new functions under the Bill. I draw the Committee's attention to the following provisions of the Bill:

- Clauses 14 and 15 provide that data holders must provide customer data to the customer or to an accredited requestor in response to a valid and properly authorised request. Clause 17 confirms that the rights created under clauses 14 and 15 do not prevent an individual from exercising their rights of access under Information Privacy Principle (IPP) 6 of the Privacy Act by making the request in some other way.
- Clause 52 provides that, where a request is made under clauses 14 or 15 and it relates to personal information, the request is not a request under IPP 6 of the Privacy Act. However, if a data holder contravenes clauses 14 or 15, or provides requested data despite having reasonable grounds to believe the request is made under duress (see clause 16(2)), the data holder's action is an interference with privacy for the purposes of the Privacy Act. The effect of this clause is that the Privacy Commissioner can investigate complaints and take compliance action in relation to such breaches.
- Similarly, clause 53 provides that, in relation to personal information, if a data holder contravenes a storage and security requirement imposed under the Bill, this will be a breach of IPP 5 of the Privacy Act.
- Clauses 144 and 145 of the Bill will amend the Privacy Act to allow the Privacy Commissioner to refer complaints to, and to consult with, the chief executive responsible for administration of the Bill.

[2] Elizabeth Kelly, *Statutory Review of the Consumer Data Right: Report*, Australian Treasury, 2022, pp. 4, 17.

The Bill includes safeguards for privacy

19. The Bill includes a number of other safeguards that will help to protect the privacy and security of personal information. They include the following provisions:

    - Clause 15 provides that a data holder must verify the identity of the requestor and confirm the customer's authorisation before providing customer data to an accredited requestor.
    - Clause 16(2) provides that a data holder must refuse to provide requested data if the data holder has reasonable grounds to believe the request is made under the threat of physical or mental harm.
    - Clauses 36 to 41 deal with customers (or secondary users acting on behalf of customers) giving authorisation to another person. Customer authorisation is required before an accredited requestor can request data from a data holder, or request that a data holder perform an action, in respect of that customer. Key features of the authorisation requirements are that:
        - authorisation must be given expressly
        - the customer must be reasonably informed about the matter to which the authorisation relates
        - the customer must be able to end the authorisation
        - authorisation must not be required as a condition of providing goods or services to a customer
        - data holders must, before providing a regulated data service in respect of a customer in response to a request from an accredited requestor, confirm that the service is within the scope of the authorisation given by the customer.
    - Clause 98(1)(d)(i) provides that, before making designation regulations for a sector, the Minister must have regard to 'the security, privacy, confidentiality, or other sensitivity of customer data and product data', and clause 99(1)(b) provides that the Privacy Commissioner must be consulted on such regulations.
    - The Privacy Commissioner must also be consulted on all other proposed regulations and standards made under the Bill (clauses 131(1)(b) and 134(1)(b)).

20. I support the requirements in clauses 131(1)(c) and 134(1)(c) for consultation with experts in te ao Māori perspectives on data, to ensure that Māori cultural perspectives and concerns in relation to data and privacy are taken into account. These requirements align with the Privacy Act's requirement that the Privacy Commissioner take account of cultural perspectives on privacy in the exercise of the Commissioner's functions.[3]

The Bill provides for information-sharing between regulatory agencies, with limitations

21. Clauses 123 to 125 authorise the sharing of information (which may include personal information) between the chief executive of the relevant Ministry and certain law enforcement or regulatory agencies (including the Privacy Commissioner). This information may be shared to assist with performing or exercising functions, powers or

[3] Privacy Act 2020, s 21(c).

duties under any legislation. The chief executive may impose conditions in relation to information provided under this part, including restrictions to maintain the confidentiality of personal information. Information provided to another person or agency under these provisions may be used or disclosed only with the authorisation of the chief executive and in accordance with any conditions imposed by the chief executive, and for the purposes of statutory functions, powers or duties.

22. I am comfortable that these information-sharing provisions are subject to appropriate limitations. I will expect the chief executive to impose relevant conditions on the use and disclosure of personal information that is shared under these provisions, to protect the privacy of individuals to whom that information relates.

Conclusions on privacy protections under the Bill

23. Taking into account the provisions of the Bill referred to above, I am broadly satisfied that the Bill establishes a CDR that includes appropriate privacy safeguards. However, there are two significant caveats to my view on the Bill's privacy protections:

    - For privacy safeguards to be effective, it is essential that my Office is adequately resourced and empowered to promote and enforce compliance with these safeguards. I return to this issue below.
    - Much of the detail of a CDR is to be spelled out in regulations and standards made under the Bill. For example, the high-level requirements for customer authorisation are included in the Bill, but the manner in which authorisation is to be given and a maximum duration for authorisation to remain valid can be specified in regulations. Until the regulations and standards have been developed, I cannot be completely sure that appropriate privacy protections will be in place when a CDR is rolled out in particular sectors.

24. In relation to the role of regulations and standards, I recognise the need for some tailoring of the regulatory regime to the contexts of particular sectors, and for technical standards to be updated as technology and business models evolve. However, I would prefer to see as much detail of privacy protections in the Bill as possible. I therefore propose that the Bill include factors that must be taken into account in making regulations and standards. In this way, the Bill could provide more clearly for privacy and other important interests to be considered in making those instruments.

25. Clause 98(1) of the Bill already specifies matters that the Minister must have regard to before recommending the making of designation regulations. These include benefits and risks relating to privacy and security of customer data. I **recommend** that the factors that the Minister must have regard to under clause 98(1) should also apply to the Minister's recommendations to make other regulations under the Bill, and to the chief executive's power to make standards.[4] **Alternatively**, if it is considered that these factors will not be appropriate for all regulations and standards, I **recommend** that the Minister and chief executive be required to have regard to privacy and security of customer data in making regulations and standards.

[4] Powers to make general regulations and standards are in part 5, subpart 9 of the Bill.

My Office's role under a CDR must be properly resourced and empowered

26. Given the importance of privacy safeguards to ensuring public trust and customer uptake of CDR opportunities, the role of the Office of the Privacy Commissioner will be key to the success of a CDR. I want my Office to play its part in helping a CDR to succeed, and this will require adequate resourcing. I would also like to see my Office's role strengthened through increased enforcement powers.

27. A recent Australian Banking Association/Accenture report on Australia's CDR highlighted low overall customer engagement with the CDR in the banking sector (banking and energy are the two sectors currently covered by Australia's CDR). At the end of 2023, only 0.31% of bank customers had an active data-sharing arrangement.[5] This report attributed low customer uptake to:[6]

    - limited compelling use cases
    - limited public awareness of CDR
    - limited underlying trust in sharing data – especially in the advent of data breaches and/or scams.

28. The report commented that:[7]

    > While the infrastructure has been built, the primary benefits will not be derived until the CDR displaces less secure data sharing options. This will require public trust and/or awareness in the system … to grow significantly.

29. With the Australian experience in mind, I want my Office to be well positioned to work with other regulators and stakeholders to build public awareness of and trust in a CDR, so that the expected benefits can be fully realised.

Resourcing

30. Funding levels and the overall funding model for a CDR are not within the Committee's remit, but it is important that the Committee understands the importance of resourcing to the success of a CDR. In addition, there is one funding issue that is part of the Bill.

31. I understand that the costs of the CDR regime that would be established by the Bill are to be met through a combination of Crown funding and funding from levies on data holders and accredited requestors. I support this approach, and my Office will need new funding from both of these sources to carry out its work effectively.

32. Clause 129(4)(b) provides for levies on data holders and accredited requestors to be used to meet some of the Privacy Commissioner's costs. Clause 129(4)(b) states that:

    > Levies must be prescribed on the basis that the following costs should be met fully out of the levies: …

[5] Australian Banking Association and Accenture, *Consumer Data Right Strategic Review*, July 2024, pp. 3, 13.
[6] Ibid., p. 25.
[7] Ibid.

(b) a portion of the costs of the Privacy Commissioner in performing or exercising their functions, powers, and duties under the Privacy Act 2020 in connection with a contravention referred to in section 52(3) or 53(1).

33. Contraventions covered by clauses 52(3) and 53(1) involve breaches of the Bill's provisions concerning customer data requests and storage and security requirements, which are to be treated as interferences with privacy under the Privacy Act.

34. Levies are to be prescribed by regulations, and the Privacy Commissioner is required to be consulted on those regulations. Levy funding for my Office will need to fairly represent the actual costs of privacy regulatory functions established by the Bill, and will need to cover a significant portion of those costs.

35. In addition to funding from levies, my Office will need new Crown funding to undertake other CDR regulatory activities. The work of my Office under a CDR will include:

- developing and publicising guidance resources for customers and businesses
- responding to privacy-related enquiries
- investigating privacy-related complaints
- receiving and advising on CDR-related privacy breach notifications
- undertaking privacy-related compliance and enforcement action
- liaising with the Ministry of Business, Innovation and Employment and other regulators about complaints and compliance issues
- providing policy advice, including statutory consultations about CDR sector designations, regulations and standards
- developing and communicating information and key messages about CDR privacy safeguards and requirements
- if necessary, developing and consulting on amendments to Privacy Commissioner-issued codes of practice that may interact with the CDR regime.

36. This list of activities represents a significant additional workload for my Office. The extent of the additional workload, and therefore the resourcing implications for my Office, will depend on the level of customer and business uptake of a CDR and the number of sectors designated under the Bill. However, there will be a base level of implementation costs for setting up new systems and processes that will apply regardless of uptake.

Enforcement powers

37. Part 4 of the Bill deals with regulatory and enforcement matters, and includes significant remedies and penalties that are not available under the Privacy Act. The differences between the penalties under the Bill and those under the Privacy Act will create a situation in which CDR breaches that do not relate directly to privacy can result in much higher penalties than privacy breaches. This discrepancy between the penalties under the two regimes will hamper the effectiveness of my Office in carrying out its CDR regulatory functions, and risks undermining public trust in the privacy safeguards of the CDR framework.

38. In particular, I note that clauses 73 to 76 provide for the making of pecuniary penalty orders of up $500,000 for an individual or $2.5 million for other contraveners (Tier 1); and $200,000 for an individual or $600,000 for other contraveners (Tier 2). These powers do not apply to contraventions under clauses 52 and 53 that are treated as inferences with privacy under the Privacy Act.

39. I do not seek to have the enforcement powers under the Bill apply to my CDR regulatory functions, as this would create a two-tier system of privacy regulation in which CDR-related privacy breaches would be subject to much greater enforcement powers and penalties than other privacy breaches. However, the difference between the enforcement powers under the Bill and those under the Privacy Act highlights the need for strengthening of the Privacy Act.

40. While this matter is outside the scope of the current Bill, I repeat the call that I have made previously for stronger enforcement and penalty provisions in the Privacy Act, including a civil penalty regime with high financial penalties to reflect the very serious impacts that major privacy breaches can have on individuals and the economy.[8] Stronger enforcement powers should be introduced to bring my Office into line with other New Zealand regulators and with my counterparts in other countries, including Australia.

The Bill should include a review provision

41. Because the Bill introduces a major new regulatory regime, I **recommend** that the Bill provide for a review to be carried out no later than three years after the first sector designation under the Bill comes into effect. The review should assess the effectiveness of the Bill and any regulations and standards made under it in achieving its objectives; and whether any changes to the regulatory regime are needed to improve the effectiveness of or safeguards under the regime. Such a review requirement was included in the Australian CDR legislation.[9]

Conclusion

42. I support the Bill and **recommend** that it be passed, with amendments.

43. I **recommend**:

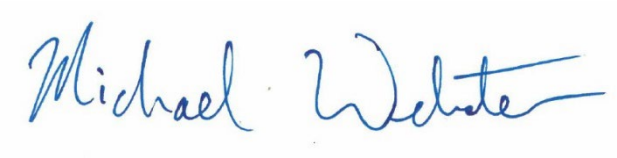
- The Bill's purpose clause be amended to more clearly refer to customers' control over their own information as a primary purpose of the Bill, and to refer to providing access to data in a way that is safe and secure. Specifically, I recommend that clause 3(2)(a) (or similar wording) be moved into clause 3(1).
- The Bill be amended to provide for matters that must be considered when making regulations and standards. Specifically, I recommend that the factors that the Minister must have regard to under clause 98(1) should also apply to the Minister's recommendations to make other regulations under the Bill, and to the chief executive's power to make standards. Alternatively, I recommend that the Minister and chief executive be required to have regard to privacy and security of customer data in making regulations and standards.

[8] Privacy Commissioner, *Briefing to the Incoming Minister of Justice*, 4 December 2023, p. 10.
[9] Competition and Consumer Act 2010 (Cth), s 56GH.

- The Bill be amended to provide for a review to be carried out no later than three years after the first sector designation under the Bill comes into effect. The review should assess the effectiveness of the Bill and any regulations and standards made under it in achieving its objectives; and whether any changes to the regulatory regime are needed to improve the effectiveness of or safeguards under the regime.

44. I trust my comments are of use to the Committee. I would like to present this submission to the Committee in person and to be available to answer any questions.

Michael Webster



Privacy Commissioner
5 September 2024