TCF Submission to the Economic Development, Science and Innovation Committee on the Customer and Product Data Bill
5 September 2024

Introduction

1. Thank you for the opportunity to comment on the Customer and Product Data Bill.

2. This submission is provided by the New Zealand Telecommunications Forum (TCF). The TCF is the telecommunications sector's industry body which plays a vital role in bringing together the telecommunications industry and key stakeholders to resolve regulatory, technical and policy issues for the benefit of the sector and consumers. TCF member companies represent 95 percent of New Zealand telecommunications customers.

3. The key issue for us in the Bill concerns the process for designation of sectors. We also comment on the following issues: requirements to become an accredited requestor, privacy, levies, implementation costs, refusing requests for data, liability issues, the relationship between the CDR and other regulation, and annual reporting.

Summary

4. The TCF supports transparency of product and customer information for consumers. As a sector we already provide customer and product data in a number of ways, as well as making it very easy to switch between providers. Competition and innovation has, and continues to, shape how customers access and are presented with and use product information. Existing regulation also helps to facilitate this.

5. We think data portability tools such as the consumer data right (CDR) can play a useful role where service providers unfairly exploit their market position or disregard user privacy and agency. This is not the case for all sectors, including telecommunications.

6. Consideration of a regulated CDR scheme should be done sector by sector. Sector analysis should include a careful assessment of the characteristics of competition in the sector, existing data access and sharing mechanisms, existing regulation in the sector, and whether benefits outweigh costs.

7. The TCF therefore recommends an addition to clause 98(1) to require the Minister to have regard to a thorough **sector analysis** before deciding to bring a sector into the regime.

8. We also recommend changes to the Bill to:

    a. Provide for a **phased and gradual approach** to designation and implementation

    b. Ensure there is **sufficient implementation time** for designated sectors

    c. Build in **statutory review**

    d. **Clarify that data holders are substantially affected** and must be consulted when regulations are made.

9. The **costs** to implement the necessary systems for a CDR regime will be considerable for designated sectors. A recently released report (commissioned by the Australian Treasury) found that costs are much higher than initial estimates from the Australian Government, with very low levels of uptake. CDR costs are likely to lead to price increases and could push smaller players out of the market and reduce competition. The Bill needs to ensure these costs are considered alongside benefits as part of the sector analysis we suggest. We recommend Committee members read the Australian Consumer Data Right Compliance Cost Review.

10. We also ask the Committee to look closely at the **privacy risks** associated with the introduction of a CDR regime. At a time when we are seeing growing concerns about data breaches and inappropriate use of data, many organisations are reducing the amount of customer data they hold and putting in place additional safeguards. Bringing in a regime that will allow third parties remote access will put data at risk. We suggest the Bill needs more rigour around the accreditation of requestors to address some of these risks. The phased approach we recommend will also help address privacy risks.

11. This submission also recommends the following amendments:

    a. **Re product data**: removing the word “ordinarily” from clause 100(2)(e) so the scope is limited to data that is publicly available.

    b. **Re liability**: including safe harbour and liability cap provisions.

c. **Re conflict of laws:** addressing the relationship between the CDR and overlapping regulatory regimes by explicitly stating that data holders who meet requirements under the Bill are protected from liability under other laws.

d. **Re grounds to refuse a request**: amending clause 16(2) to make grounds of threat or harm a discretionary requirement, and expanding the scope in clause 16(1) to allow refusal of requests where disclosure of the data would likely result in fraud and if providing the data requested would expose the data holder to breach of other laws.

e. **Re charges**: amending clause 32 so that regulations concerning charges in connection with regulated data reflect the differing nature of each sector, the type of data request, and the associated costs on data holders in complying with the regime.

f. **Re levies:** amending clause 129(2) to remove data holders.

g. **Re reporting**: removing the obligation in clause 112 that data holders report annually to MBIE on complaints (and any matters specified by regulations), or alternatively amending clause 112 to enable reporting via a sector wide dispute resolution scheme.

Designating sectors

One size does not fit all

12. The designation process in the Bill makes it possible for any customer-facing sector to be brought into the CDR regime. However, all sectors are not starting from the same point. Careful consideration is therefore required before making a decision on the designation of sectors that already share customer and product data and make it easy to switch between providers, such as telecommunications. Especially where such sectors have high levels of competition, and are already regulated for competition and consumer purposes (in our case by the Commerce Commission).

13. The Government's work on the CDR regime was sparked by issues in the banking industry. An approach designed to address open banking issues should not be applied economy wide, without taking into account differences between sectors, existing regulations and levels of competition. The legislation needs to allow for flexibility, review and consultation before any decisions about designation are made to help ensure the resulting framework is workable and proportionate.

Telecommunications customer and product data

14. The telecommunications sector is very competitive. With around 150 retailers, consumers have many providers to choose from. Month to month plans and number portability make it easy to change providers.

15. Number portability statistics show that a high level of switching is taking place. Every week the industry handles almost 10 000 porting events.

16. The appendix to this submission provides further information on telecommunications and customer and product data, including:

    a. The various codes of practice the telecommunications industry has in place to help consumers switch providers, understand and compare product offerings, understand usage, and choose the right plan for their needs.

    b. Commerce Commission initiatives and existing powers that have a similar policy intent to the CDR, for telecommunications.

Sector analysis should be undertaken before bringing sectors into the regime through the designation process

17. We are very concerned that important questions about who will be subject to the CDR regime are being left to regulation, without a requirement to do regulatory impact analysis. While ministers and officials have been considering the issues relating to banking for a number of years, this analysis has not been done for sectors such as telecommunications.

18. We appreciate the Bill requires the Minister to have regard to certain matters before designation regulations are made. This includes important things such as the interests of customers, the likely costs and benefits for data holders, and security, privacy, confidentiality and intellectual property matters. But this is not enough.

19. The TCF submits that clause 98 be amended to also require the Minister to commission and have regard to a thorough sector analysis, in line with the Government Expectations for Good Regulatory Practice, before any decision is made to bring a sector into the regime. This view is in line with other submitters' views on the 2023 exposure draft, including Business New Zealand, who recommended a comprehensive and in-depth investigation prior to sectors being designated.

20. The sector analysis should consider:

    a. the stated objectives of the proposed designation

    b. the characteristics of competition in the sector

c. whether consumer protections and broader consumer welfare would be advanced, including consideration of privacy concerns

d. existing data access and sharing mechanisms and whether these, or other options, could meet the policy intent

e. existing regulation that requires the sharing of customer and product information, and whether this could meet the policy intent

f. the likely benefits or positive outcomes and costs or negative outcomes of the proposal (a designation should not be able to proceed unless there are net benefits for New Zealanders).

21. The analysis should be done in meaningful consultation with the data holders in the sector concerned, with opportunities to workshop issues and make submissions (we make further comments on the consultation provisions in the Bill later in this submission). Any existing regulators should also be involved. This will help ensure better outcomes for customers and a workable regime for the affected sector.

22. Without the requirement for a robust sector analysis Parliament would be delegating power to apply obligations to a sector without sufficient regulatory impact analysis being done. We submit that the list of considerations currently contained in the Bill is not sufficient to meet the Government Expectations for Good Regulatory Practice.

Australian experience supports the need for sector analysis

23. The Australian experience supports the argument for robust sector analysis, and is evidence of the need to tread carefully and take time with the designation of sectors.

24. The Australian Government reversed its decision to bring telecommunications into its CDR regime (it will reassess again at the end of 2024 when there has been more experience with banking and electricity). While the Australian Treasury was able to quantify costs (discussed below) it was not able to adequately estimate the value of the benefits. Policy work was paused for two years.

25. A recently released independent review of compliance costs associated with the Australian CDR revealed the complexity of the Australian regime and found that each industry needs to be considered separately to avoid unnecessary costs and unintended impacts for consumers in that industry.

26. New Zealand can benefit from the fact that countries, such as Australia and the UK, are further advanced in the development of their respective CDR regimes and can apply the lessons learned if it takes a phased approach (as suggested below).

A CDR will be high cost - existing approaches may be less costly for consumers

27. Considering existing mechanisms and regulation in a sector (as part of a sector analysis) could identify less costly mechanisms to achieve the policy intent compared to applying the CDR regime to a sector. This would be a win for consumers.

28. The costs associated with the CDR regime are considerable, and will result in increased overheads and ultimately higher prices for consumers. Increased costs could also limit capacity for innovation and strategic investments.

29. One of the most significant costs to the telecommunications industry (if designated) will come from establishing the required electronic system, getting it to talk to many other systems in an existing business, and complying with the technical and other requirements under regulations and standards (for example, for APIs and verifying consent). Each sector will have to start from scratch in developing these systems, because of sectoral differences (which will also need to be taken into account in regulations).

30. In 2021 the Australian Treasury estimated the costs of implementing a CDR for the Australian telecommunications industry as follows:

    a. For large companies, build costs of around A$4.3 million, with A$1.28 million per year in running costs, per provider.

    b. For small services providers, build costs of A$340 000 and per year running costs of around A$160 000, per provider.

31. The above cost estimate did not include related digital transformation projects to update legacy IT systems. It also assumed outsourced service providers would be available to support data holders to efficiently comply with CDR obligations.

32. A recent independent review of compliance costs associated with the Australian CDR found:

    a. **Costs have far exceeded the original regulatory estimates**. The implementation costs for many data holders (including small players) has been in excess of A$1 million, ranging up to over $100 million for bigger organisations. This is for a regime that does not yet cover action initiation (which is proposed for the New Zealand CDR).

    b. **The level of usage of the CDR has been low,** leading many to question whether benefits outweigh costs. A review undertaken by the Australian Banking Association and Accenture in July supports this finding. The Accenture study found that 0.31 percent of Australian banking customers are

using the CDR, with banks having invested $AU1.5 billion to implement the regime so far.

33. We agree that the Australian Treasury calculations undervalued the costs, especially for API development and small providers. In a sector of around 150 retailers, many of them small, this would be a barrier to entry. A number of existing smaller operators would struggle or be unable to continue to operate, reducing competition and consumer choice. Larger telcos have hundreds of systems that would require costly changes in order to enable the use of APIs envisaged.

34. Negative competition impacts are being seen in Australia. The Australian Banking Association reports that implementation costs have been disproportionate, with mid and low tier banks incurring disproportionately higher compliance costs compared to major banks. The Association notes this has negatively impacted competition, contrary to the CDR's intent. This Australian study also found the CDR compliance costs were leading to vital technology and customer projects being deprioritised (including digital banking experiences and scam detection and prevention).

35. We recommend Committee members read the Australian Consumer Data Right Compliance Cost Review, and Accenture's Consumer Data Right Strategic Review.

A phased and gradual approach to designation and implementation

36. In addition to adding more rigour to the designation process by requiring sector analysis, we also submit the Bill be amended to require the Minister to take a phased approach that enables the regime to be implemented gradually.

37. In practice, this would mean sectors are designated one at a time, with a sufficient gap between designations for a proper assessment and cost-benefit analysis to be carried out (including the sector analysis proposed above) and any lessons learned from preceding sector designations to be applied for future designations.

38. Other forms of phasing to consider include:

    a. Starting with read only, not action initiation

    b. Starting with accredited third parties, followed by customer direct access.

39. Action initiation is of particular concern. It was not initially included in the Australian regime, but is currently being considered. There are concerns on both sides of the Tasman about complexity and error handling with action initiation. In scenarios where a customer's data could be passed through multiple intermediaries it will be very difficult to audit and manage when errors and incidents happen. If New Zealand takes a staggered approach it can wait and see how action initiation plays out in Australia before deciding whether or how to go ahead.

40. A staggered approach will be beneficial for both data holders (enabling implementation costs to be staggered) and consumers (a more thought out and better functioning regime will provide stronger consumer protection).

Implementation timeframes for designated sectors

41. When sectors are designated, it will be essential to ensure there is sufficient implementation time to allow designated sectors to make appropriate system and process changes. The Bill should require the Minister to consult with the sector to determine an appropriate implementation time frame. When implementing new regimes it can help ease the compliance burden by introducing phasing or transitional arrangements so that no one is unnecessarily burdened by immaterial technical non-compliance.

Statutory review

42. The Bill does not provide for a statutory review or review cycles. We recommend that a statutory review period is included in the primary and secondary legislation, requiring periodic targeted reviews of designated regimes in place. Given the potential imposition of cost on new sectors, we also recommend that such reviews occur before designating other sectors.

43. Requiring a statutory review period helps ensure the design of the CDR regime is fit for purpose and improvements can be efficiently made to accommodate differences and required updates. It will also ensure that, where the costs and benefits no longer stack up, these can be addressed.

44. We note a statutory review is consistent with feedback the Ministry of Business Innovation and Employment received in 2023 on the exposure draft. [1]

Consultation with data holders when making regulations and standards

45. Clauses 99, 131 and 134 require the Minister to carry out consultation on regulations or standards with persons who will be 'substantially affected'. This drafting creates uncertainty as to who exactly will be consulted, given potential ambiguity as to who will be "substantially affected" in certain contexts. The Bill should be explicit that data holders within each relevant sector must be consulted. This could be achieved by amending clauses 99(1)(a), 131(a) and 134(a) by adding at the end of each clause: "including all data holders within the relevant sector."

46. In addition, clause 99(4) states that 'a failure to comply with this section does not affect the validity of the designation regulations.' This provision potentially

[1] BusinessNZ Submission, page 10, Business NZ: Submission on the Customer and Product Data Bill (mbie.govt.nz); Mercury Submission, page 1, Mercury: Submission on the Customer and Product Data Bill (mbie.govt.nz);

undermines the importance of the consultation process by allowing the Minister to bypass the consultation process without any consequences, and should therefore be removed. The Government needs to avoid creating a potential pathway for regulations to be developed without adequate consultation with data holders and other key stakeholders.

Definition and scope of data

47. Our submission on the exposure draft of the Bill raised concerns about derived and value added data being in scope, and the chilling effect this could have on investment in data analytics and innovation. We see there has been an attempt to address this concern by providing that data holders do not have to share product data that is not ordinarily publicly available. We support this approach in principle but submit that the word "ordinarily" be removed from clause 100(2)(e) so the scope is limited to data that is publicly available.

Accreditation and privacy risks

48. At a time when we are seeing growing concerns about data breaches and inappropriate use of data, many organisations are reducing the amount of customer data they hold and putting in place additional safeguards. Bringing in a regime that will allow third parties remote access will put data at risk. This is why the Bill needs to put in place robust safeguards for accreditation.

Requirements for accreditation should be in the Bill

49. The Bill leaves too much of the detail concerning accredited requestors to be determined by regulation. We think the primary legislation needs to include some base requirements that could be added to using a regulation making power at a later date.

50. We recommend the following requirements for accreditation be considered:

    a. being a fit and proper person

    b. demonstrating information protection and security measures

    c. being certified to hold and store large amounts of personal information

    d. demonstrating that the purpose for which they will use data is ethical and aligns with the legislation

    e. demonstrating the value of the service they are seeking to provide to consumers (to sift out requestors who may be seeking to take advantage of consumers)

f. evidence of appropriate insurance.

MBIE should assess and verify certain matters

51. The Bill should include functions for MBIE as the regulator and administrator of the scheme to assess and verify that accredited requestors have adequate information and protection measures and are certified to hold and store large amounts of personal information. MBIE should also regularly check that accredited requestors are adequately protecting data and providing the service they promise to consumers. Given the risks involved a self report would not be sufficient.

Relationship to information privacy codes

52. We have unresolved questions (posed during the exposure draft process) concerning how the CDR requirements will sit alongside existing obligations our sector has under the Telecommunications Information Privacy Code, a code of practice established under the Privacy Act by the Privacy Commission. The Code covers telecommunications information collected, held, used and disclosed by telcos. It includes getting consent for information collected, and obligations when providing information to a third party. Other sectors also have information privacy codes. We suggest the Committee seeks advice on this issue and shares it with submitters.

Liability issues

Safe harbours

53. Unlike the Australian legislation, the Bill doesn't protect firms that are complying with regulation in good faith from civil or criminal liability through the provision of safe harbours. MBIE looked at this in submissions on the draft bill and concluded that clauses 16, 18 and 20 gave sufficient protection from liability. We do not agree, as there are risks not covered off. For example, the very fact of opening up an interface to company systems puts data holders at risk of mis-use or fraudulent behaviour that could cause harm. Westpac's submission on the exposure draft talks to this matter more fully.

Liability cap

54. The liability cap (for where providers fail to comply with any regulation or standard) included in the exposure draft has been removed. This is a problem, because the complexity of the CDR system and likely changing standards[2] means it could be

[2] The independent review of CDR compliance costs in Australia found (page 3) that standards have changed many times, causing problems. To illustrate the pace of change, since the CDR 'went live' with data sharing in mid-2020, there have been: three major reviews of the CDR framework; 16 consultations on legislative and regulatory changes; 20 versions of the binding CDR data standards; and over 100 formal proposals for changes to the standards.

several weeks or months before a data holder knows they are not compliant. We submit there needs to be a cap or at least some sort of narrowing of the parties or scenarios where losses can be claimed.

Relationship between the CDR regime and other regulation

55. The telecommunications sector operates in a highly regulated environment (see appendix for further information about telecommunications regulation). We are concerned about the potential overlap between the regulatory regime in the Bill and existing regulation designed to promote competition and protect consumers. Examples of overlap include the retail service quality regulation undertaken by the Commerce Commission, and the information privacy codes developed by the Privacy Commissioner.

56. This issue isn't limited to existing regulation. For example, at the same time the Committee was calling for submissions on the Bill, the Commerce Commission was consulting on a very similar regime for banking, and has made recommendations to the Minister for Commerce and Consumer Affairs to designate the interbank payment network under the Retail Payment System Act.

57. The relationship between the CDR and overlapping regulatory regimes needs to be addressed in the Bill. If this is not done there will be significant uncertainty for data holders. Without clarity, data holders are likely to face materially increased complexity and compliance costs, as well as potentially overlapping liability under different frameworks.

58. The Bill should address this by stating explicitly that data holders who meet the requirements under the Consumer and Product Data Bill are protected from liability under other laws, provided their actions are compliant with the CDR framework.

Refusing requests for data

59. Clause 16 sets out the circumstances when a 'data holder may or must refuse requests for data', including that data holders 'must refuse to provide any data requested under either of those sections if the data holder has reasonable grounds to believe that the request is made under the threat of physical or mental harm'.

60. While we understand the desire to protect consumers from harm, this is not a practical requirement in our view. Telecommunications companies are not (and should not be expected to be) qualified to identify when customers may be under the threat of physical or mental harm unless this is somehow expressed by the customer. We also don't see how such an assessment could be practically carried out in the context of an electronic and automated system for granting data requests.

61. To address the above problem we submit that clause 16(2) be amended to make refusal on grounds of threat of harm a discretionary requirement, by changing the drafting from 'must' to 'may'.

62. We also propose that clause 16(1) be expanded to allow data holders to refuse requests for data in additional circumstances, including where the data holder reasonably believes that disclosure of the data would likely result in fraud and if providing the data requested would expose the data holder to breach of other laws.

63. The Committee might also consider whether that addition of a ground for refusal for frivolous and vexatious requests would work in a system where requests are made via APIs. Section 18(h) of the Official Information Act and section 53(b) of the Privacy Act include "frivolous or vexatious" as a ground for refusing a request.

Fees that can be charged by data holders

64. Clause 32 provides for regulations to be made concerning charges in connection with regulated data services, covering matters such as the amounts that can be charged and caps on charges. It is important that the consultation process the Government engages in to determine these charges considers (and then reflects in the resulting regulation) the differing nature of each sector, the type of data request, and the associated costs on data holders in complying with the regime. We submit that clause 32 (1)(a) be amended to include this requirement.

Levies and funding the CDR regime

65. We submit that levies should only apply to businesses who stand to benefit commercially from accessing data from designated sectors. These businesses will be gaining value from the data of designated sectors, and designated sectors will have to meet the significant costs of introducing new systems and complying with the requirements of the regime. To this end, we recommend removing data holders from clause 129(2) of the Bill.

66. We also note that the Australian CDR (the model New Zealand is looking to follow) receives significant funding from the Australian Government, which has spent a considerable sum to get its CDR regime up and running. This includes:

    a. The $AU 111.3 million earmarked in the 2021/22 Federal Budget to "accelerate the roll out of the CDR"

    b. The allocation of a further $88.8 million over the next two years to support the continued operation of the consumer data right across the banking, energy and non-bank lending sectors[3].

[3] https://www.cdr.gov.au/rollout

67. If the New Zealand Government wishes to implement a successful regime it will need to consider government funding for its establishment and operation, and how this spending stacks up against other government priorities.

Annual reporting of complaints by data holders

68. Clause 112 requires annual reporting about complaints by data holders to the Chief Executive of MBIE. We question the utility of this requirement where industry dispute resolution schemes already have reporting requirements as part of their current business models.

69. We submit that clause 112 be amended to remove the obligation that data holders report annually to MBIE on complaints (and any matters specified by regulations). Alternatively, clause 112 should be amended to enable reporting via a sector wide dispute resolution scheme where one exists. The Chief Executive of MBIE would receive a copy of the annual report from the industry dispute resolution scheme, rather than reports from individual data holders. This will help avoid duplication and unnecessary compliance costs.

70. Any reporting should only concern valid complaints which go through to the relevant industry dispute resolution scheme.

Contacting the TCF about this submission

71. Please contact kim.connolly-stone@tcf.org.nz in the first instance if you have questions about this submission.

Appendix: pre-existing regulation and initiatives for telecommunications

Telecommunications regulation already provides for data sharing and switching

1. The regulatory regime for telecommunications already requires a significant amount of data and information sharing, as outlined below. Much of this is designed to make it easy for consumers to compare what is on offer and easily switch between providers.

Industry self regulation

2. As part of its self-regulatory function, the TCF develops and administers a range of codes and activities to support consumers on behalf of the telecommunications industry. This includes:

    a. Number portability: the TCF manages and administers the Industry Portability Management System on behalf of the industry. This system allows consumers to retain their mobile or home phone number when they switch provider.

    b. The Product Disclosure Code: this code is mandatory for TCF retailers and specifies what information service providers must make available to customers about their broadband plans, performance and traffic management in a standardised way, enabling consumers to easily compare product offerings across providers. This Code is scheduled to be reviewed later this year, with further standardisation of product information to be implemented.

    c. The Mobile Plan Information Framework: developed by industry to standardise a minimum set of mobile plan information made available by mobile providers to third parties for the purposes of developing mobile comparison tools, such as Mobile Compare.

    d. In 2021, mobile providers took steps to increase transparency of mobile usage and spend information to their customers, aimed at helping consumers to choose the right plan for their needs. Providers are continuing to deliver improvements in this area, with the Commerce Commission recently recognising the industry's efforts and concluding that further regulatory intervention is not required at this stage[4].

[4] https://comcom.govt.nz/__data/assets/pdf_file/0025/354562/Addressing-transparency-and-inertia-issues-in-the-residential-mobile-market-update-Open-letter-6-June-2024.pdf

e. Customer transfer codes for fibre and copper services: these codes describe the process that must be followed when consumers switch their service from one service provider to another.

3. It would be necessary to review existing codes in light of the CDR, at considerable cost.

Commerce Commission initiatives and existing powers have a similar policy intent

4. Under the Commerce Commission's retail service quality programme, the Commerce Commission published an emerging views paper on product disclosure which sets out six measures for improving the ability of consumers to compare products, plans, providers and mobile coverage. For example, recommending standard average monthly prices, improving transparency of cost disclosure to customers, and a consistent approach to how GST is displayed. This work aligns with the policy intent of CDR to improve customer access to their data and standardise data for the purposes of plan and product comparison.

5. There is a risk that a CDR would duplicate existing Commerce Commission powers and work on retail service quality.

[ends]