TCF Submission to the Ministry of Business, Innovation and Employment
On the exposure draft for the Consumer Data Right
24 July 2023

Introduction

1. Thank you for the opportunity to comment on the June 2023 exposure draft and discussion document on setting standards and safeguards for customer and product data exchange.

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 TCF supports transparency of product and customer information for consumers. While we support the general concept of a consumer data right (CDR) scheme, we are of the view that it should not have economy wide application unless careful assessment of consumer welfare, the characteristics of competition in the sector, and a cost benefit analysis, is done sector by sector.

4. The key issues for us from the exposure draft and the discussion document concern the designation of sectors. We also raise issues concerning derived and value added data, privacy, costs, levies, banking APIs and dispute resolution.

Telecommunications customer and product data

4. In this part of our submission we outline the ways the telecommunications industry already provides customer and product data. This kōrero is to show that all industries are not starting from the same point in their data sharing journey. It provides the

evidence base for later points in our submission about the design of the CDR and the designation of sectors in particular.

Telecommunications regulation already provides for data sharing and switching

5. The regulatory regime for telecommunications already requires a significant amount of data 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.

6. 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 consistent way, enabling consumers to easily compare product offerings across providers. This Code is scheduled to be reviewed later this year.

    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, aiming at helping consumers to choose the right plan for their needs.

    e. Customer transfer codes for fibre and copper services: these codes describe the process that must be followed when consumers switch service providers.

    f. The use of homogenous language, in customer facing information, to describe products and services.

7. We also have 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.

8. We have questions for MBIE concerning industry privacy codes:

a. Can you please explain how the Telecommunications Information Privacy Code might be impacted if the CDR was to apply to telecommunications?

b. As the proposed CDR covers some of the same ground, will the Privacy Commissioner be expected (and resourced) to review and update industry codes?

Telecommunications providers already use online tools and apps to share usage information with customers

9. The telecommunications sector already makes it really easy for customers to get information about their usage through online tools and apps.

Commerce Commission initiatives and existing powers have a similar policy intent

10. 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.

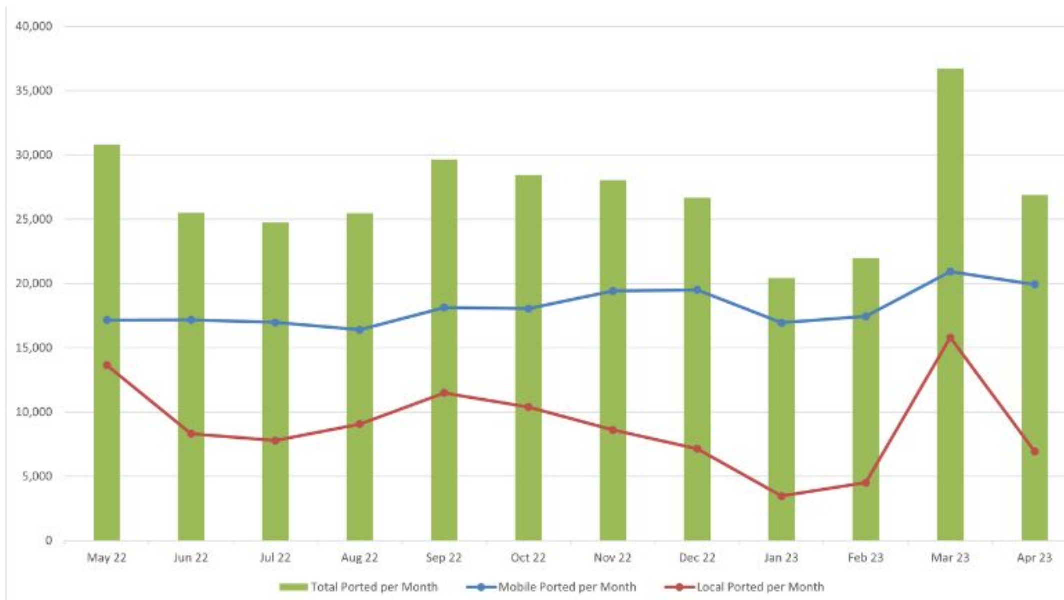
11. The retail service quality programme, combined with existing Commerce Commission powers, shows there is already considerable focus on data sharing in the telecommunications sector.

12. There is a risk that a CDR would duplicate existing Commerce Commission powers and work on retail service quality. A regulation making power enabling the application of a CDR to telecommunications would be double jeopardy.

Telecommunications is already a very competitive industry

13. The telecommunications sector is already very competitive. Consumers have many providers to choose from. Month to month plans and number portability make it easy to change providers.

14. Number portability statistics show that a high level of switching is taking place. Every week the industry handles almost 10 000 porting events. The chart below shows the number of mobile and local ports per month.



15. Commerce Commission market monitoring data shows that 27 percent of residential consumers have switched providers in the past year alone. A further 965 000 customers changed their plan. This equates to over 50 percent of customers taking action to change their provider or plan in the past year alone. With such high levels of engagement, a CDR regime is unlikely to drive material change in the telecommunications sector.

Bringing other sectors into the regime

16. MBIE's work on the CDR regime was sparked by issues in the banking industry. What we see in the exposure draft is an approach intended to address open banking issues, with an assumption that it can work economy wide if sufficient flexibility is provided in regulation making powers.

17. There is a risk that sectors that are designated later in the CDR process will be assessed against rules or standards that are specific to the banking industry and are unconnected with those sectors, or that go further than is needed to meet CDR objectives for data sharing and competition. We make three recommendations on how to mitigate this risk:

    a. Provide more certainty through the designation regulations on how other sectors will be assessed for inclusion in the regime (discussed below).

    b. If the Government wants to move quickly to address issues in the banking industry, enact the legislation so that it applies to banking, but delay the coming into force of the designation regulation making power for two years,

so that MBIE (in consultation with affected industries) has time to consider the potential impact of a CDR regime on other industries.

c. Build in a statutory review period, requiring a review of the (primary and secondary) legislation and its initial application to banking, before government considers designating additional sectors. We are also conscious that technology and industry practices concerning data sharing will move relatively fast, making review and updates desirable. Another possible outcome of a review could be to remove sectors that had been designated where the costs and benefits no longer stack up. We think a statutory review period is needed because MBIE would be doing ongoing policy work as well as implementing the regime.

18. It would also be helpful if MBIE produced and shared a timetable setting out the sectors it is seriously considering as candidates for the CDR and the order in which they would be considered.

19. The Australian experience is evidence of the need to tread carefully and take time with the designation of additional sectors. Australia recently reversed its decision to bring telecommunications into its CDR regime. While the Australian Treasury was able to quantify costs (discussed below) it was not able to adequately estimate the value of the benefits. The work has been paused for two years.

Requiring a sector analysis as part of the regulations designating additional sectors

20. While it can be tempting or convenient for government to leave matters concerning the designation of future sectors for regulation or standard making powers down the track, we think it is preferable to include some details in the legislation rather than leaving them open.

21. We recommend that the **regulation making power for future designations** (in clauses 60, 61 and 62) be amended **to require a thorough sector analysis before any decision is made to bring an additional sector into the regime.** The sector analysis should be undertaken in consultation with the sector concerned. In addition to the cost benefit analysis contemplated in clause 60(1) (b), the assessment should consider:

    a. the characteristics of competition in the sector

    b. whether consumer welfare would be advanced

    c. a thorough analysis of existing data access and sharing mechanisms and whether these, or other options, could meet the policy intent

d. existing regulation that requires the sharing of customer and product information.

22. Without this requirement Parliament would be delegating power to apply obligations to a sector without sufficient regulatory impact analysis having been done.

Concerns re the definition and scope of data

Derived and value added data

23. The exposure draft takes a very open ended approach to what data could be covered by the regime. Data is defined as including information, customer data means data about an identifiable customer, and designated customer data means data that is specified in the data holder designation regulations.

24. Sectors that could be affected by the regime need certainty (to guide investment decisions) that the regulations will not cast the net too wide in terms of the scope of the customer data that will be included. The exposure draft makes no mention of derived data and value added data. If derived and value-added data can be included, this will have a chilling effect on investments in data analytics for the telecommunications sector (and other sectors), which would spill over into the data analytics industry. This would have the opposite effect of what is intended, by reducing innovation and flow on benefits to consumers. We therefore submit that derived and value added data should be expressly excluded from the definition or regulation making power.

25. The regulatory impact statement (RIS) for the CDR considered the issue of derived data, noting that including it in the CDR could deter businesses from developing new methods of analysing data in the provision of products or services, which could have flow on impacts for consumers. The RIS also acknowledged that if derived data relates to an identifiable individual it is likely to be considered personal information for the purposes of the Privacy Act, so is already available to consumers.

Privacy

26. We are concerned that MBIE has not fully considered the privacy risks of the proposed CDR and weighed these up against the potential benefits. 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 information they hold and putting in place additional safeguards. Bringing in a regime that will allow third parties remote access to data seems counterintuitive to this societal concern.

Consent settings

27. We think the discussion document has not appreciated the complexity of the task of checking consent (in clause 33 and 34) for data holders. We would need to take a very thorough approach with considerable cost. Government work on digital identity has struggled with this issue, with recent budgets failing to provide funding to progress the work.

28. We also note that consent settings may need to differ sector to sector. For example to take into account the amount of access to customer data that is already available.

Accreditation

29. The exposure draft leaves too much of the detail concerning accredited requestors to be determined by regulation at a later date. Given that accredited requestors will be dealing with large amounts of consumer data, it is important that the primary legislation (clause 65) include minimum requirements. A regulation making power could be retained to add additional matters at a later date.

30. The discussion document asks for views on the requirements for becoming accredited. We agree with the suggested requirements concerning fit and proper person, demonstrating information protection and security measures, evidence of appropriate insurance and supporting the participation of Māori. We recommend that MBIE also consider two additional requirements:

    a. That accredited requestors be certified before they can hold and store large amounts of personal information.

    b. That applicants demonstrate the value of the service they are seeking to provide to consumers. This would help to sift out requestors who may be seeking to take advantage of consumers.

31. We also have questions for MBIE about who will ensure that accredited requestors have robust information protection and security requirements. Given the risks involved it does not seem sufficient to allow a self report. It will also be important that the regulator regularly check that accredited requestors are adequately protecting data and providing the service they promise to consumers.

Costs of complying with a CDR regime

32. The most significant costs to the telecommunications industry (if our sector is designated for a CDR) will come from establishing the electronic system envisaged in clause 26, 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).

33. The Australian Treasury has estimated the costs of implementing a CDR for the Australian telecommunications industry as follows:

    a. For small services providers it estimates build costs of A$260 000 and ongoing costs around A$160 000, per provider.

    b. For larger companies the build costs are estimated at around A$1.4 million, with A$1.28 million ongoing costs.

34. We think the Treasury calculations undervalue the costs, especially for API development and small providers.

35. The costs of developing APIs are of particular concern. In a sector of over 90 retailers, many of them small, this would be a barrier to entry. A number of existing smaller operators would 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 in the discussion doc. We consider the MBIE question concerning banking APIs later in this submission.

36. We are also concerned that the CDR will increase overheads resulting in increased prices for consumer products and services. This would come at a time when government is also proposing to increase costs for critical infrastructure for resilience and other purposes across a range of sectors including telecommunications, with consumers inevitably expected to bear at least a portion of those costs. All of this in the context of a cost of living crisis. It is therefore essential that a thorough cost benefit analysis is done for each sector.

37. If less costly mechanisms can be found to meet the policy intent, that will be a win for consumers. This is why we have recommended a robust process for considering whether additional sectors come into the regime, which looks at existing initiatives in a sector and other options.

Levies

38. The discussion document notes that government will cover its costs through the imposition of levies and accreditation fees.

39. We submit that any levies should only apply to businesses who stand to benefit commercially from accessing data from designated sectors. These businesses would already have gained value from the data of designated sectors, and designated sectors will have borne the significant costs of introducing new systems and complying with the requirements of the regime.

Will banking standards work for telco?

40. Question nine of the discussion document asks “other data holding sectors” which elements of the Payments NZ API Centre Standards are suitable for use in other sectors, and which could require significant modification.

41. An assessment of banking APIs and their applicability to telecommunications and other sectors is a major exercise. This is something that MBIE needs to resource and provide adequate time for. We would welcome a presentation from MBIE and relevant experts.

42. In the meantime we note that the Australian assessment was that proposed banking standards would need to be adapted quite fundamentally for telecommunications. For example, to address the fact that telecommunications already has number portability (while banking doesn’t), the way accounts are set up, and different security requirements.

Dispute resolution

Using existing industry schemes

43. The exposure draft provides that data holders (and accredited requestors) will need to have a customer complaints process. The discussion document talks about requiring the use of existing industry schemes. It goes on to talk about non-privacy complaints regarding breaches of the law’s obligations being dealt with by existing industry dispute resolution schemes within the designated sector. MBIE suggests that the designation regulations require both data holders and accredited requestors to be a member of the relevant industry dispute resolution scheme. Question 35 seeks views on the above issues.

44. The TCF supports the above proposal. The telecommunications industry has recently updated its dispute resolution scheme - the TDR. We support data holders and accredited requestors being required to be members of the relevant industry dispute resolution scheme. For telecommunications that scheme is the TDR.

Triaging complaints

45. While we support using existing industry schemes, we are concerned that the current drafting is not clear enough on where consumers should first initiate a complaint and who triages whether it is a matter for the Privacy Commissioner, the industry dispute scheme or MBIE. The diagram on page 54 of the discussion document assumes that a customer will know who to go to with their complaint. We think the process needs to include an initial triaging point.

Annual reporting of complaints by data holders

46. We question the utility of the requirement in clause 63 of requiring annual reporting on complaints to the Chief Executive of MBIE by each dataholder. This seems unnecessary when industry schemes already have reporting requirements as part of their business as usual.

47. If the Chief Executive of MBIE really does wish to see such reporting, we recommend it only be for valid complaints which go through to the relevant industry dispute resolution scheme, who can provide specific reporting for their sector. We suggest that the Chief Executive of MBIE receives a copy of the annual report from the industry dispute resolution scheme, rather than reports from individual data holders. This would be easier for everyone.

Contacting the TCF about this submission

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