SUBMISSION TO PRODUCTIVITY COMMISSION:

DATA AVAILABILITY AND USE DRAFT REPORT

ANZ

12 DECEMBER 2016

Executive Summary

1. ANZ thanks the Productivity Commission for the opportunity to contribute again to the Commission's inquiry into data availability and use. As with our submission on the Commission's issues paper (**Issues Paper**), our contribution largely concerns the availability of private sector data.

2. For the reasons given under 'Introductory Comments' below, ANZ is supportive of the Commission's recommendation that consumers have an economy-wide 'Comprehensive Right' to access and transfer their 'consumer data'.

3. Our specific suggestions on how the recommendations could be improved are as follows:

   - **Define 'consumer data' carefully** – The Commission's proposed definition of 'consumer data' is a broad one and would capture identifiable data while excluding de-identified data. We have four concerns with this definition.

     - **First**, data thought de-identified may be easily rendered identified through relatively simple manipulation and analysis. Thus, the belief that data is '…demonstrably not able to be re-identified…' could be illusory and reflective only of the current data custodian's intent and capability. As such, the definition may not provide the most certain foundation for the Comprehensive Right.

     - **Second**, the definition would capture data that has been the subject of substantial analytical investment (eg insights concerning a specific individual). The transfer of such highly transformed data to a third party and in due course, its assignees, would be a fillip to those parties that would undermine the original data custodian's commercial interests. This may disincentivise investment in data collection and development and seems an inapt foundation for competitive markets.

     - **Third**, and related to our second concern, we would question whether all identifiable data needs to be subject to the transfer right to encourage competition. Within financial services, comparison and alternative service providers only need raw transaction and account data, coupled with product attribute data, to understand how consumers have historically behaved and recommend and provide competing products. Other identifiable data, such as a data custodian's proprietary analytical insights concerning individual customers, are superfluous to this objective.

- **Fourth**, the expansive definition could capture data that data custodians may be legally or practically unable to deliver to the consumer. For example, certain 'consumer data' held by a data custodian may actually be the intellectual property of another entity and legally non-transferable by the data custodian under current law. Any definition of 'consumer data' will need to be cognisant of these limitations.

To address these concerns, we would suggest that the Commission define 'consumer data' as encompassing an individual's transaction (or consumption) data only, at least for the transfer right (this would include account balance data for banks). The Commission could explore a tiered definition of 'consumer data' under which a broader definition is applicable to other limbs of the Comprehensive Right.

- **Provide a regulatory framework that safeguards data** – We believe that the Comprehensive Right should be supported by a regulatory framework that ensures transferees of 'consumer data' meet minimum data security, privacy and consumer protection requirements. This will ensure that consumer faith in open data access is preserved and provide an objective certification regime for identifying competent data recipients. The regulatory model established by the European Union's 2015 *Payment Services Directive* (**PSD2**) provides an example of such a framework.[1]

  As a segue to our third point, we would suggest that the Commission adopt an approach of a top-down regulatory framework for safeguarding data with a bottom-up, industry-led approach to the technical means of providing access to that data.

- **Initiate a process to establish the legislative framework and work through technical and legal issues** – An open data regime will involve myriad complex technical, regulatory and legal issues that stakeholders, industry and Government will need to work through. These issues include, but are not limited to, protocols for authenticating requests for data access, the liability regime that will attach to data transfers, the appropriate regulatory body and framework and the intellectual property issues associated with data and databases.

[1] *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC* (**PSD2**).

For example, we would suggest, as we did in our submission on the Issues Paper, that stronger rights concerning data drawn from databases would allow data custodians to protect their investment while still allowing consumers to benefit from greater access under a Comprehensive Right.

We'd also strongly suggest that industry be allowed flexibility in determining the most appropriate data delivery mechanisms. Legislatively enshrining one mechanism over others could constitute a significant opportunity cost. A bottom-up approach to the development of technical standards would allow industries and private entities to adopt the most appropriate technology to meet the Comprehensive Right.

On timing specifically we'd note that, while PSD2 and the UK's open bank regime are scheduled to commence in 2018, the legislative framework and preparatory work are much more advanced in those jurisdictions than here.[2]

[2] The latest UK development has been the publication of a draft order from the Competition and Markets Authority that would establish a body to develop standards and designate particular entities as being require to provide access to certain data sets. See Competition and Markets Authority, *Retail Banking Market Investigation Draft Order – Consultation* 'The Retail Banking Market Investigation Order 2017' available at: https://assets.publishing.service.gov.uk/media/5835888e40f0b614ff00000a/retail-banking-draft-order-for-consultation.pdf

Introductory Comments

4. ANZ supports the Commission's position that consumers across the economy should have greater access to data. Just as data can underpin the commercial success of companies, data can underpin confident and informed decision making by consumers. Most hopefully, data on historical product and service usage (ie transaction data) could inform product and service purchasing decisions, empowering consumers to make better choices and boosting competition between providers.

5. Further, the legally underwritten access to data afforded by the Commission's proposal for a 'Comprehensive Right' may also help engender consumer faith in the collection and use of data by private sector entities. Privacy and security will be critical issues in an open data world. ANZ believes that addressing these issues appropriately will be a pre-requisite to the success of Australia's digital economy.

6. ANZ also continues to believe that economically successful access reforms will be those that carefully calibrate the effect that such access has on the commercial position and incentives of entities that invest in generating, collecting, organising, protecting, analysing and making available data (termed **data custodians**).

7. With the right policy settings, this interplay between consumer empowerment, consumer faith and commercial interests will be more mutually reinforcing than zero-sum. To restate our submission on the Issues Paper, if individuals trust third parties to protect their data, then they will be more likely to share data. If data custodians can have their commercial interests protected, they are more likely to invest in the generation, protection and availability of data. If more data can be made available, then consumers (and thus society) may benefit.

8. Reiterating another point from our submission on the Issues Paper, we'd note that voluntary initiatives towards opening up data to consumers and generally are already occurring absent reforms. Beyond the instances of data sharing that we highlighted in that earlier submission, ANZ also has an emerging open application programming interface (**API**) strategy and has been working with APIs to provide data to our wholesale customers.[3] Further, as discussed below, ANZ is

[3] In our submission on the Issues Paper, we noted that:

ANZ makes financial data available to customers to assist them with managing their finances. For example, customers can download transaction data in common formats to their computers. Business customers are able to register so that automatic, direct bank feeds of transaction data are sent to customers' compatible

participating in industry-based discussions concerning open data. We look forward to further discussions.

9. That said, ANZ believes the Commission's recommendations for reform are fundamentally well directed towards encouraging further data access while balancing consumer empowerment, consumer faith and commercial interests. Coupling the vesting of a 'Comprehensive Right' in consumers to access data with an initial preference for industry-led means of access is a neat solution to the challenge of catalysing additional action while avoiding the potential pitfalls of top-down development of technical standards. As noted above, additional reforms to provide regulatory protections to consumers and underpin commercial interests in data investment would complement the Comprehensive Right.

10. Lastly, ANZ supports the Commission's premise that the Comprehensive Right apply to all consumer data through the economy. Consumers should have the ability to aggregate their data from diverse data custodians. It is possible to imagine data aggregation and/or comparator services providing single views of consumer's energy, telecommunications, grocery and banking consumption patterns and options. Such a service would be less feasible with a limited application of the Comprehensive Right.

11. Our comments on the specific recommendations are set out below. We have prepared these comments cognisant of the recommendation by the House of Representatives Economics Standing Committee that banks be required to provide open data access through APIs by July 2018 (**House Recommendation**).[4]

accounting software packages. ANZ has set up direct bank feeds with a number of accounting software providers to make reconciling business accounts easier. This service is available at no cost to customers.

[4] Parliament of the Commonwealth of Australia *Review of the Four Major Banks: First Report* (November 2016), xviii.

Comments on Recommendations

Draft recommendation 4.1 – Comprehensive Credit Reporting

12. We have few concerns with the Commission's recommendation on comprehensive credit reporting (**CCR**).

13. We would, however, suggest that the Commission:

- Clarify that the 40% threshold applies at the industry level, rather than at the individual contributor level; and
- Recommend the Office of the Australian Information Commissioner and/or the Australian Securities and Investments Commission lead discussions on resolving concerns with the reporting of repayment history information (**RHI**). ANZ is ready to report RHI and would welcome discussions under the aegis of a body that could clarify the regulatory position on this topic.

Draft recommendation 6.2 – Industry standards for data access and Application Programming Interfaces (APIs)

14. ANZ supports the Commission's draft recommendation that the private sector is likely to be best placed to determine sector-specific standards for data sharing. This bottom-up approach to development will allow the economy the flexibility to adopt the most suitable technology today and in the future.

15. We believe that the private sector would be sufficiently incentivised to develop data sharing mechanisms through the Comprehensive Right. As with the experience of the Open Bank Working Group in the United Kingdom, there is a valuable role for industry to play in developing standards concerning data access and sharing. Through the Australian Payments Council, ANZ has already started exploring opportunities to work with industry partners to determine financial industry-specific standards.[5] We believe that more could be done in this vein.

16. We note that the Commission seeks more information on the benefits and costs of a legislative presumption in favour of providing data via APIs. As recounted above, the House Recommendation is that banks must provide data via APIs by July 2018.

17. We would suggest that the main issue with a legislative presumption for APIs is that such diminished technical latitude could constitute a significant opportunity

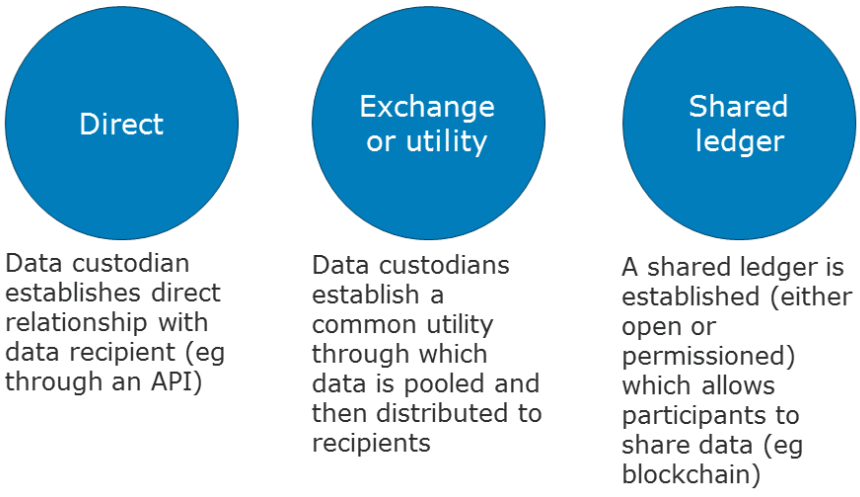
[5] Australian Payments Council *Annual Review 2016*, 9; available at: http://australianpaymentscouncil.com.au/wp-content/uploads/2016/11/Australian-Payments-Council-Annual-Review-2016.pdf

cost for the economy; it may dissuade or prohibit the private sector from pursuing alternative and more effective data transfer mechanisms either initially or in the future. For example, distributed ledger technology (aka blockchain) is an emerging means by which data can be shared, while the New Payments Platform will allow more data to be sent with payments.

18. As the Commission considers whether to recommend such a legislative presumption, we would ask it to consider recommendation 39 of the Financial System Inquiry that Government '[e]mbed consideration of the principle of technology neutrality into development processes for future regulation.'[6] While the Financial System Inquiry also recognised that common technology standards could be beneficial in certain cases, we believe that the appropriate mechanism by which data is shared could vary with industry, data-type, recipient and, of course, technological developments.[7] We would anticipate that large private sector entities would ultimately deliver upon the Comprehensive Right using a range of technologies, depending on the data recipient, data-type and competitive bent of the entity.

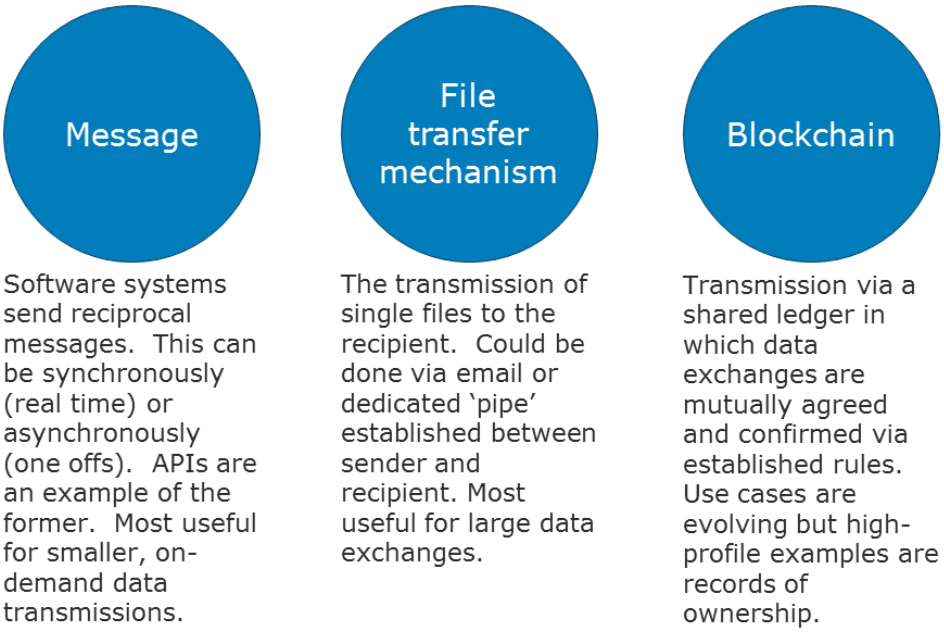
19. We have set out below some of the current design considerations for data sharing. These considerations are across the data sharing model, the technical transfer mechanism and the format of the shared data. There would be other considerations concerning security and governance arrangements. As is evident, the decision of how to share data through an economy is not a binary one between API and file transfer but a multifactorial one.

- **Data sharing model** – this refers to how data sharers and recipients are organised.



[6] The Australian Government the Treasury *Financial System Inquiry Final Report* (2014), 269; available at: http://fsi.gov.au/files/2014/12/FSI_Final_Report_Consolidated20141210.pdf.
[7] Ibid, 270.

- **Data sharing mechanism** – this refers to the technical means by which data is transmitted from one entity to another



- **Data format** – the form in which data is shared. Examples include comma separated values (CSV), excel formats, PDFs and picture files.

20. Thus, while direct APIs are clearly beneficial for frequent, individual and real-time data transfers, file transfer mechanisms may be more apt for large scale, one-off transfers. Further, we believe there is merit in considering not just direct data sharing models but data exchanges. These could be particularly useful for situations where data need to be shared among identified entities while spreading a number of governance, technical and security costs across participants.

21. As such, we do not think that legislatively presuming that direct APIs are apt for all elements of Australia's data sharing regime is appropriate. As noted above, we think the existence of the Comprehensive Right, coupled with the prospect of Government intervention if effective industry-based initiatives do not materialise, will be sufficient to catalyse the development and implementation of effective technical solutions to the challenge of data access.

22. The main financial costs associated with the data access will likely attach to the antecedent and collateral steps to the actual delivery of the data. These costs would include:

    - The substantial internal engineering required to identify, collect and organise for delivery the data sets requested by consumers on an industrial scale. For data custodians with multiple engagement points with consumers, this may mean ensuring diverse technology systems can be scoured and relied upon to

deliver up homogenized data packets that meet specified standards. Data custodians would need to embed redundancy in their systems to ensure the Comprehensive Right can be met when invoked. The cost of this work would increase as the definition of 'consumer data' broadened (see discussion below).

- Related to this, data custodians would need to assess their capacity to process large volumes of data feeds, particularly if the Comprehensive Right were to be crafted to capture constant (also known as 'synchronous') data feeds, rather than one-off deliveries.
- The governance framework controlling any form of data transfer to external entities would need significant initial and ongoing investment. Data custodians would need to develop an effective mechanism to verify consumer authorisation, the correct data set and the identity of the recipient as nominated by consumers exercising the Comprehensive Right. Verification would need to cover both the dispatch and receipt of data. Legal certainty concerning the liability of data transfers, as discussed below, would help alleviate some of this governance cost.

23. While it is difficult to ex ante determine the cost to an organisation of providing data to its customers, we would estimate that combining the steps above with the actual development costs of a relatively simple transfer mechanism, like an API, would be in the tens of millions of dollars. Such cost would vary with parameters such as the scope of data being delivered, delivery method and the security framework required. More formal arrangements, like a data exchange utility, could involve higher development and maintenance costs. Of course, the costs of a utility could be spread over its users.

Draft recommendation 9.1 – Introduction of a definition of 'consumer data'

24. The Commission has proposed a broad definition of 'consumer data' that establishes a dichotomy between 'identifiable' and 'de-identified' data sets. The former set would be captured by the definition, subject to the Comprehensive Right and include all data through which an individual can be identified. The latter set would be the converse of the former.

25. We note that the House Recommendation is that banks provide access to customer and small business data.[8] This would include '…for example, customer's transaction history, account balances, credit card usage, and mortgage repayments.'

[8] House of Representatives, above n 4, 42.

26. Like the Commission in respect of financial services, the House Committee has also identified product attribute data (i.e. the '…terms and conditions for each of their banking products in a standardised and machine-readable format') for release.[9]

27. While ANZ favours more consumer empowerment than less, it would ask the Commission to consider whether its draft definition of 'consumer data' is well directed towards achieving a balance between consumer empowerment, consumer faith and commercial interests that ANZ believes should be the policy goal of Australia's data access reforms.

28. We have four specific concerns with the currently proposed definition. These concerns do not apply to the concept of product attribute data.

29. **First**, the definition rests on what can be the relatively permeable distinction between identifiable and de-identified data. As the Commission notes itself, there are substantial difficulties with concluding that de-identified data cannot be re-identified.[10] Motivated organisations and technological developments may undo de-identification steps and thus move data back within the definition of 'consumer data'. For example, location data drawn from social media could be matched with, and thus re-identify, transaction data. Similarly, within the organisation that collected the relevant data, the distinction between identified and de-identified data may simply rest on the organisation's intent.

30. The uncertain nature of this delineation between identifiable and de-identified data could raise fraught legal and technical issues. For example, if it was discovered that data hitherto thought de-identified were somewhere rendered identified (or identifiable) through mistake, technological development or third party interference, would the Comprehensive Right attach itself automatically? As such, we do not think the proposed definition of 'consumer right' provides a solid foundation for the Comprehensive Right.

31. **Second**, the definition would capture data that has been subject to significant manipulation and investment by a data custodian to generate commercially valuable insights concerning individual consumers. For banks, this could include individual internal credit scoring and assessments for offers. While it is conceivable that a consumer may benefit from accessing this data, its transferral to a third party and its assignees in competition with the data custodian would be a clear fillip to those parties. This would undermine the legitimate commercial

[9] Ibid.
[10] Productivity Commission *Data Availability and Use, Draft Report* (2016), 198.

interests of the original data custodian and erode a basis of competitive differentiation. It may also be contrary to the terms and conditions pursuant to which third parties provide such data to data custodians.

32. As we discussed in our submission on the Issues Paper, we believe it is essential that investment in data is respected. We stated:

> *Data custodians would be legitimately concerned from a commercial and equity perspective if policy settings concerning data did not recognise [data's] value and cost. If data custodians are not able to capture the benefits of their investment in data, then they will have less incentive to make such investment.*

33. **Third**, and related to the second point, we believe that consumers could benefit from increased competition even with the right to transfer a more limited scope of data. If one of the main objectives of data availability is to allow consumers to use their data to compare and acquire alternative services and products, then this could be achieved with transaction data. This would include an individual's purchases, payments (including automatic payments) and balances. Such data could be used to understand historical consumption patterns and, through this, optimal future services and products. Of course, an individual's static data, like name and address may also be useful to an individual in moving between different service providers. Other identifiable data, such as a data custodian's analytical insights, would be superfluous to this objective.

34. **Fourth**, the expansive definition could capture data that data custodians may be legally or practically unable to deliver to the consumer. For example, certain 'consumer data' held by a data custodian may actually be the intellectual property of another entity and legally non-transferable by the data custodian. Similarly, some data held by data custodians may be in forms that are not amenable to easy transfer to third parties (eg paper or within legacy systems). Further, there are current limits on how long entities need to retain data. We would suggest that 'consumer data' not capture all data that has been created by a data custodian but rather existent data held by the data custodian.

35. Equally, some data sets that would be captured by the currently proposed definition of 'consumer data' could relate to national security or financial system integrity. Accordingly, data flagging an individual for illegal activity would ostensibly be caught. Allowing an individual to access this data before investigations or reporting to, and actions by, authorities have been carried out could jeopardise the ability of banks and Government agencies to address such illegal activity appropriately. Any definition of 'consumer data' will need to be cognisant of these limitations.

36. **To address these concerns**, we would suggest that the Commission consider a more constrained definition that captures just transaction and static data. For example, we note that the United Kingdom's Competition and Markets Authority (**CMA**) has recently released a draft order entitled *The Retail Banking Market Investigation Order 2017*.[11] This proposes mandating that certain UK account and small-to-medium lending service providers provide access to specified data sets that are much more narrowly and precisely defined than either the Commission or the House Committee is recommending.

37. Specifically, under this draft order, providers must provide read access to product and reference data concerning personal current accounts (**PCA**), business current accounts (**BCA**) and small-to-medium enterprise lending products (including unsecured lending and commercial cards), and read/write access to transactional data concerning PCA and BCA products. While the CMA's definitional approach would not work on an economy-wide basis, it is a useful reference point in considering data scope issues.

38. The Commission may also like to consider a tiered definition of 'consumer data' that matches different data sets with the various limbs of the Comprehensive Right. Thus, the definition proposed above may be matched with the transfer limb of the Comprehensive Right while a broader right may be matched with the access and review limbs.

39. Beyond the conceptual issues with the definition of 'consumer data', we would urge the Commission to consider recommending crisp and clear definitional wording from the outset. While there may be evolutionary merit in allowing the content of the phrase 'consumer data' to be filled in through competitive interpretation and iterative judicial consideration, certainty of the definition's ambit would provide a solid foundation for the industry's initial access initiatives and allow attention to be placed on how, rather than what, to deliver to consumers.

Draft recommendation 9.2 – Individuals should have a Comprehensive Right to access digitally held data about themselves

40. As stated above, ANZ supports the bestowal of a right on individuals to access and transfer their data and thus agrees with the Comprehensive Right in principal. We note that the transfer element of the Comprehensive Right is analogous to the House Recommendation.

[11] Above n 2.

41. The transfer limb of the Comprehensive Right would clearly bolster consumer empowerment and competition within the Australian economy, as noted above. In addition, the rights to access data, be informed about intended transfer or sale and appeal automated decisions would underpin consumer faith in a similar way that pre-existing cognate rights under the *Privacy Act 1988* (Cth) (**Privacy Act**) already do.

42. We have **seven** key observations that the Commission may like to consider as it finalises its recommendation for a Comprehensive Right.

Access, request edits and be informed of transfer

43. **First**, as noted, the limbs of the Comprehensive Right concerning access, editing and being informed of transfers are similar to pre-existing rights under the Privacy Act. As such, the Commission and Government will need to carefully consider the relationship between the Privacy Act and any new data-related legislation to ensure there is no overlap or conflict between the legal regimes. This is to ensure clarity of legal rights and obligations and minimise regulatory burdens.

Appeal automated decisions

44. **Second**, the Commission has proposed that consumers be allowed to appeal automated decisions. We appreciate that this concern arises in a world where more decisions are being made by algorithm.

45. However, we would be concerned if this right allowed consumers to challenge the substantive outcome of such decisions, rather than just the accuracy of the data inputs to those decisions. We believe that the ability to challenge substantive outcomes would undermine commercial entities' freedom to contract and risk manage their exposures, as well as increase their costs, with potentially little benefit to consumers. We note that right to correct the accuracy of data would likely be captured by the Commission's proposed right to request edits to data.

46. Automated decisions by large entities are reflective of their desire to contract with others. The decisions are predicated on clearly defined policies. For example, a bank's automated decisions concerning the extension of loans are digital applications of the policy that sets out the bank's lending criteria. These lending criteria are crafted to meet responsible lending obligations, risk manage the bank's exposures and achieve commercial outcomes. We would be concerned if the right allowed consumers the ability to force a second guessing of these criteria.

47. Further, even if the right simply allowed a consumer the ability to have an individual remake the algorithm's decision *de novo*, it is unlikely that the individual would be given any more latitude. They would still need to make a decision within the policy's parameters. As such, we would question how often this would produce a different result. Providing such a right may simply add significantly to entities' costs without changing substantive outcomes for consumers.

48. Separately, the Commission may like to consider which decisions are appropriately captured by the appeal right. Some automated decisions within banks, for example, are taken to flag and report suspicious transactions to authorities. Banks would need to be able to act on such decisions without facing rights of appeal so as to allow the information to be reported to the authorities in a timely and confidential manner. Thus, we would submit that the appeal right needs to be carefully crafted to underpin consumer faith without undermining the public interest.

Direct data holders to copy data in machine-readable form, either to the individual or to a nominated third party

49. Our remaining **five comments** are on this proposed limb of the Comprehensive Right.

50. **Third**, the proposed Comprehensive Right seeks a world wherein consumer data will flow freely from data custodian to data custodian at the direction of the consumer entitled to the data. Recipient data custodians will then be able to transfer or sell that consumer data, subject to compliance with any laws. We believe that to ensure this schema operates without endangering consumer faith, privacy and cyber-resilience protections will need to apply across data custodians.

51. Presently, consumer data held by banks is subject to stringent requirements to ensure its protection from theft and misuse. With the advent of the Comprehensive Right and/or implementation of the House Recommendation and without further reform, such consumer data would be transferred to and held by entities that are not banks and potentially not subject to the same data protection requirements.

52. This raises inherent and serious concerns about individuals' data. Data breaches concerning an individual could risk their financial security and wellbeing, particularly through identity theft. While public attitudes towards data availability may be liberalising, this does not change the underlying threat that misappropriated data can cause significant financial harm.

53. It also raises the risk that a major data breach at a lightly regulated entity will undermine consumer faith in all financial service providers. In a fintech world, consumers may not distinguish between highly regulated banks and lightly regulated non-banks; a failure at an entity drawn from the latter category may taint all.

54. We do not think that these risks could be adequately mitigated by warning consumers that the entity to which they wish their data to be transferred is less regulated than the transferring data custodian. Expecting all consumers to understand the personal implications of the differential regulatory treatment of data custodians may be a bridge too far.

55. We would suggest that the Commission considers an appropriately calibrated regulatory regime for recipients and holders of consumer data to ensure they meet minimum standards concerning data. Such standards would consider topics such as data security and recovery, privacy, remediation of and consumer redress for data breaches and sales and transfers to third parties.

56. Such a regime would have two outcomes. First, it would protect consumers (and thereby the economy) from data breaches. Second, it would allow data custodians transferring data to third parties to identify those recipients which are authorised and competent to receive the data.

57. To support our point, we would direct the Commission's attention to the PSD2 regime. This establishes a regime under which account information providers (ie entities which access certain bank data and provide services based on it) need to be authorised and subject to risk management requirements.[12] Thus, while PSD2 establishes a framework of liberalising data (and payment services), it does so within a regulatory framework that supports data security and privacy.

58. **Fourth**, and related to our prior point, we believe that it will be essential that the Commission consider how to protect consumers from entities exploiting behavioural biases to accept default settings and not interrogate terms and conditions upon signing up for online services. Consent from a consumer for a provider to access their data held elsewhere may be given cheaply or without reflection. While that may be the consumer's prerogative, it may also allow the unscrupulous to flourish and, over time, erode consumer faith in the ideal of free data.

[12] PSD 2, above n 1. See Article 11 for the authorisation requirement; Article 95 concerns risk management requirements.

59. Thus, the Commission may like to consider minimum standards for the acquisition of consumer authority for the transferral of data. Again, PSD2 is instructive. Article 94(2) provides that payment service providers can only '….access, process and retain personal data necessary for the provision of their payment services, with the *explicit consent* of the payment service user' (emphasis added).[13]

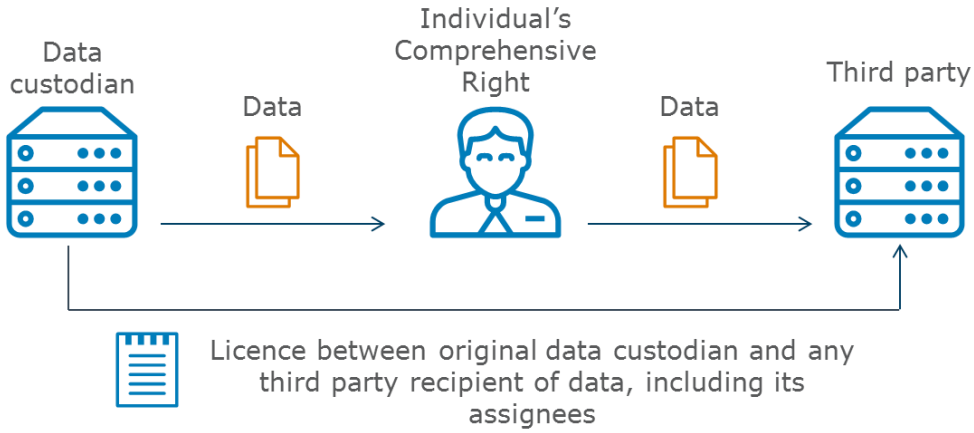
60. **Fifth**, we would encourage the Commission to consider the liability of data custodians transmitting data on behalf of a consumer. For data to flow freely, we would suggest that data custodians need certainty that, provided they follow certain defined steps in responding to a consumer's request that the custodian transfer the consumer's data to another, they will be absolved from data breaches and other losses that arise from the transfer, use or reliance upon the data. Such losses could arise, for example, if the recipient of the data is fraudulent, negligent or mistakenly identified by the consumer. Nor should data custodians be liable for errors in data: They should only be required to be provide data on an 'as is' basis. Appropriate safe harbours for data transferors could be incorporated in the Commission's proposed *Data Sharing and Release Act*.

61. **Sixth**, we continue to believe that there are important intellectual property issues that need to be addressed to better underpin data availability. As discussed in our submission on the Issues Paper, the current law on copyright provides imperfect protections to data drawn from databases (eg where replication of a database is not 'substantial' or the data ceases to be part of a 'literary work'). Such imperfect protection, coupled with the inherent limitations of contract law (which only controls rights and obligations between the contracting parties), would mean that once data custodians transfer data to a third party commercial recipient and, critically, its assignees, they would have limited means of protecting their legitimate commercial interests.

62. Recognising a *sui generis* 'database right' in this form of data would allow data custodians to license data with recipients while not interfering with the Comprehensive Right. As the Commission has suggested, data custodians and consumers could have shared rights in data. This could operate in accordance with the diagram we offered in our earlier submission.

[13] Ibid, Article 94(2).

How data could be shared using database right



63. **Last**, we believe it is important that data custodians are afforded sufficient time to be able to deliver against the Comprehensive Right. PSD2 and the UK process for open bank data are notionally scheduled to commence in 2018. We would note that this commencement date rests on a foundation of substantial preparatory work which is yet to be completed in Australia (eg legislative framework, regulatory consultations and industry agreement on standards). Further, as discussed above, the CMA's draft order concerns a much more limited set of data than contemplated by either the Commission's recommendations or the House Recommendation. Thus, we would suggest that there are significant limitations with taking the UK and EU timing for data access as the benchmark for Australia. In this light, we would encourage the Commission to consult widely concerning the appropriate timing of the commencement of the Comprehensive Right once its form (including the definition of 'consumer data') is clarified.

Draft recommendation 9.4 – Establish a process whereby public and private datasets are able to be nominated and designated as National Interest Datasets (NIDs).

64. ANZ supports the greater availability of data through the economy and would welcome access to greater amounts of data currently held by Governments.

65. The success of this recommendation with respect to private datasets will hinge on the judicious designation of such datasets as NIDs. As we noted in our submission on the Issues Paper, banks, like ANZ, already make substantial datasets available through public and regulatory reporting. We would be concerned if the NID designation process were used to compel banks to deliver datasets outside these existing reporting parameters.

ENDS