SUBMISSION TO PRODUCTIVITY COMMISSION:

ISSUES PAPER: DATA AVAILABILITY AND USE

ANZ

29 JULY 2016

Executive Summary

Introduction

1. ANZ thanks the Productivity Commission for the opportunity to contribute to the Commission's inquiry into data availability and use. Our contribution concerns the availability and use of private sector data.

2. Information technology sits at the core of ANZ's banking strategy. We invest around $1 billion annually developing in our capabilities. This investment reflects our optimism about the benefits that data and the digital economy can bring to our customers. Our customers increasingly demand digital services that make intelligent and respectful use of the data that we hold on them. ANZ's recent launch of Apple Pay and Android Pay for ANZ card holders is a strong example of how banks can use new digital channels to meet emerging customer demand.

3. Appropriate policy settings concerning private sector data will help us and our peers meet this demand. We already make a substantial amount of data available. We believe that more will become available without policy reform due to competitive pressures and initiatives already underway. If, however, the Commission is minded to recommend reform, we think that it should consider creating a new database right, similar to that existing in the European Union. This new right, which would protect investment in data and databases beyond current copyright law, would encourage the private sector to further invest in data and then make it available. We believe this would facilitate greater data availability more effectively than mandatory requirements.

Structure of submission

4. To help the Commission understand our position, this submission has two parts.

5. **First**, we set out some background on how data is currently used in banking. In this section, we identify that ANZ is investing heavily in digital banking services. We also make significant amounts of data available to our customers, shareholders, regulators and others for commercial and legal reasons.

6. **Second**, we set out our thoughts concerning policy settings that could encourage data availability. These thoughts are broadly in response to the Commission's questions concerning private sector data and consumer data.

Policy settings

7. With respect to these policy settings, we believe that the current regulatory framework coupled with advances in technology is already encouraging financial services businesses to make significant amounts of data available. ANZ and other businesses are working through complex privacy, commercial, security and other issues as we seek to make more data available, including through comprehensive credit reporting (**CCR**).

8. If the Commission is of the view that reform is needed, we believe that there are three interests in data that policy settings need to recognise and align in order for data to benefit Australian society and the economy:

   - The interests of individuals in their own privacy and dignity with respect to data concerning them that private sector actors hold.
   - The commercial interests of those who invest in generating, collecting, organising, protecting, analysing and making available data (termed **data custodians**).
   - Society's interests in the benefits that could arise from greater availability of private sector data.

Bundle of rights

9. Recognising these interests and fostering the sharing of data is best achieved through ensuring that the bundle of rights which attaches to data provides sufficient, balanced protections for each interest and encourages voluntary data sharing. Mandating the availability of data carries a number of risks which potentially undermine all three interests.

10. The current bundle of rights attaching to data, including those rights originating in the *Privacy Act 1988* (Cth) (**Privacy Act**) and *Copyright Act 1968* (Cth) (**Copyright Act**), appears to protect individual interests well. We acknowledge, however, that protecting individual interests is critical in a data-driven world.

A new right in databases

11. That said, this bundle of rights is not perfect. Current copyright law gives incomplete protection to data in databases (eg where replication of a database is not 'substantial' or the data ceases to be part of a 'literary work'). Without adequate protection, and particularly in a situation where data availability was mandated, data custodians would be unable to recoup investment in data

generation, integrity and availability. This would disincentivise investment beyond the minimum needed to service customers.

12. As such, and on the basis that copyright law is not amended, it would be valuable to introduce a new right vested in data custodians concerning databases and the data housed therein. This new right, similar to that introduced in the European Union in 1996, would allow data custodians to licence data that they hold in databases for use by third parties. This would allow them to benefit from investment in the generation, protection and increased availability of data. In turn, this would allow higher volumes of quality data to be available for uses that benefit society.

Data in Banking

How ANZ uses data

13. Digital technology and data capability is central to ANZ's competitive strategy and business. Our CEO announced at the ANZ May 2016 results that a superior digital services experience for customers is one of our four key priorities. Highlights from the announcement include:

    - ANZ was the first major bank in Australia to offer Apple Pay (note: since the results we have also announced that we offer Android Pay).
    - Over 1.3 million customers are using the mobile banking application goMoney. goMoney provides a wide range of banking services such as account transfers and BPAY® for iPhone and Android. $72b of transactions are processed annually using goMoney.
    - The identities of 65% of customers applying for savings accounts online have been verified using the ANZ Digital Identity Verification system.
    - We are achieving high levels of customer satisfaction over our mobile banking channel (92% in Australia, 99% in New Zealand).

14. ANZ invests approximately $1bn annually on digital projects. ANZ's digital projects fall into five areas:

    - Digitisation and customer experience - creating a consistent customer experience across physical and digital channels, analytics and data
    - Service and product processing - systems and process standardisation, consumer lending capabilities and payments networks
    - Stability and security - improving resilience against attacks (including associated risks of breach of privacy relating to customer data), and infrastructure stability
    - Product enhancement - product and service improvements, re-engineering of divisional products
    - Risk - minimising operating risks, meeting regulatory and customer expectations

15. We have a particular focus on delivering a high quality, consistent and secure customer experience across multiple channels. This requires developing a multi-channel digital platform and migrating existing services on to that platform. The information system architecture is being developed particularly to support mobile

banking, including providing application programming interface services to ANZ partners.

16. 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 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.[1]

17. We undertake extensive data analysis to improve our services and products. Customer contact and product information is used to improve services across channels, manage product life cycles and set pricing. Customer information is central to credit risk, funding and lending practices. We monitor transaction data to protect the security of customers. For example, we track where and when purchases are being made and, if there is an inconsistent pattern of transactions, contact customers to check for fraud.

18. ANZ is working with partners from industry, academia and government. Our work with these partners focuses on the customer and employee experience; distributed ledger and blockchain; big data, machine learning and advanced analytics; digital workforce; and cyber security. We are seeking to develop an open environment for innovation that is accessible to our partners, reduces time to market and effectively manages intellectual property rights, risk and security.

19. ANZ is:

    - Collaborating with Australian and regional universities to test how emerging technology and research can be applied to banking (for example, advanced security, mobility, analytics, visualisation and process simplification).
    - Participating in building the New Payments Platform, which will allow increased amounts of data to be sent with payments.[2]
    - Engaging with fintechs, venture capital companies and related companies. We have partnerships with the York Butter Factory in Melbourne, and Stone and Chalk in Sydney. ANZ's 'Data Science Hackathon' with the York Butter Factory' focused on data driven insights for beef, grains and dairy trade. The 'Digitise ANZ Ops' weekend with Stone and Chalk aimed to identify

[1] http://apps.anz.com/internet-banking/help/update-details/bank-feeds/
[2] http://www.apca.com.au/about-payments/future-of-payments/new-payments-platform-phases-1-2

opportunities to improve customer service and productivity in ANZ operations in the region.

- Working with major global vendors, including on developing new tools and databases to improve our data analysis.
- Working on Hyperledger, a collaborative project seeking to develop an open source solution to financial challenges.[3]
- Contributing to key government programs such as the national cyber security strategy, and related intelligence and defence measures. We are partnering with the eSafety Commission and Microsoft to improve cyber safety practices in the community.
- Exploring additional technology to assess credit applications and potentially collections decisioning.

20. Security and fraud protection is a core bank capability. Every day, ANZ tracks the use of hundreds of thousands of devices connected to our network; for example mobile devices, servers, employee workstations and business and home computers. We work closely with other banks, and Australian and other government agencies. As is widely acknowledged, the sophistication and expertise of digital criminals continues to grow.

Existing regulatory requirements concerning data availability

21. Like other Australian banks, ANZ is subject to a number of regulatory requirements to make data available.

22. ANZ and other Australian banks have invested heavily to meet regulatory obligations. The Australian Bankers Association surveyed the four major banks and three regional banks about the cost of major regulatory related information system changes to assist the Financial System Inquiry.[4]

23. The survey showed that the seven banks have allocated $1.73 billion for implementation of the eight selected projects since these projects commenced, with Anti-Money Laundering related changes the most costly at $725 million and Foreign Account Tax Compliance Act at $234 million.

[3] https://www.hyperledger.org/

[4] Australian Bankers' Association *Financial System Inquiry Response to Interim Report* (August 2014), 64; available at: at http://fsi.gov.au/consultation/second-round-submissions/ .

Privacy Act and Comprehensive Credit Reporting

24. The principal current regulatory requirements concerning data are those of the Privacy Act and its *Australian Privacy Principles*. These requirements will be well known to the Commission.

25. For the banking sector, the Privacy Act is also the source of the requirements concerning CCR. This is set out in Part IIIA of the Privacy Act.

26. CCR establishes a voluntary scheme under which credit providers and credit-reporting bodies can share and receive credit-related information. For credit providers, like banks, the provisions in Part IIIA generally apply in addition to the *Australian Privacy Principles*.

27. To facilitate CCR, Part IIIA sets out the regime under which bodies collect, store, use and share credit-related information. Due to the sensitive nature of credit-related information, Part IIIA sets out stringent requirements for subject entities to follow in dealing with that information.

28. Importantly, these provisions restrict the use to which credit-related information can be put by both credit providers and credit-reporting bodies. For example, section 21D prescribes when a credit provider can disclose credit information to a credit-reporting body.

29. As noted in our submission to the Financial System Inquiry, ANZ supports CCR and is making a significant investment in its reporting capabilities. We expect to be providing and receiving CCR data in 2017-18. ANZ estimates that on the basis of current plans the cost to the banking industry of fully implementing CCR will be between $400 and $500m.

30. Our current view is that mandating CCR would be premature given the substantial amount of in-flight activity. Delays in implementation have been driven by a range of factors, including complexity, differing views of legal requirements and levels of assurance that are needed for handling such sensitive personal information.[5] The Commission should wait to see if the current activity results in enhanced levels of reciprocal sharing of credit data before it considers further regulatory intervention.

[5] For example, a recent Financial Ombudsman Service decision highlighted how credit providers could have different understandings of the reporting requirements. In this case, the credit provider reported an account as past due while a temporary arrangement was in place (in accordance with a requirement to continue to age the delinquency), but the determination also required them to report that the customer was up to date with their payments. The decision is available at this link: https://forms.fos.org.au/DapWeb/CaseFiles/FOSSIC/422745.pdf

E-Payments Code

31. Another important element of the regulatory framework concerning banks is the E-Payments Code.[6] This is a voluntary code that concerns electronic payment facilities. It is administered by the Australian Securities and Investments Commission (**ASIC**). ANZ is a subscriber to the code.

32. Under the code, ANZ (and other bank subscribers) must give customers a list of direct debit, direct credit and periodical payment arrangements for the last 13 months upon request (see clause 35). This is to help customers switch banks.

33. The information that banks must provide includes the payment details of the arrangements (eg payee, amount, payment dates, type of arrangement).

34. Clause 35 of the code also allows customers who are switching to a new bank to ask the new bank to obtain a list of payment arrangements from their current bank. The current bank must provide this to the new bank.

35. Separately, under clause 12 of the code, users of electronic payment services may not provide pass codes (eg pins, passwords) to anyone, unless the user makes a reasonable attempt to protect the security of the pass code. This is to help protect the integrity of the payment facility provided to the user. This would prevent a user giving access to a third-party service to access the data held within an electronic payment service that is provided to the user.

Product and services disclosure

36. The attributes and features of ANZ's products and services are currently publicly disclosed in accordance with the disclosure requirements of Chapter 7 of the *Corporations Act 2001* (Cth) (**Corporations Act**).

37. While such disclosure has typically manifested in printed documents and PDF versions of those documents, ASIC has recently liberalised its disclosure requirements to facilitate greater use of digital mediums.[7] We expect that this liberalisation, coupled with customer demand, will push many financial services firms to provide more and more product and service attribute disclosure through these mediums. This will mean that this information will more easily be discoverable.

[6] http://www.asic.gov.au/for-consumers/codes-of-practice/epayments-code/

[7] Australian Securities and Investments Commission *Regulatory Guide 221 Facilitating Digital Financial Services Disclosures* (March 2016); available at: *http://download.asic.gov.au/media/3798806/rg221-published-24-march-2016.pdf*

Financial data – Pillar III disclosure and Basel Committee Quantitative Impact Studies

38. In addition to making information concerning the bank available via our shareholder reporting (for example, our annual report and ASX continuous disclosure), ANZ makes significant amounts of data concerning its financial position available in compliance with its Pillar III reporting obligations.

39. Pillar III reporting obligations are set by the Australian Prudential Regulation Authority (**APRA**) for banks.[8] They largely concern banks' prudential capital and liquidity position. Our Pillar III disclosure is available on our website.[9]

40. Further, ANZ, like many internationally active banks, makes a significant amount of confidential financial data available to APRA under periodical quantitative impact studies. These studies are driven by the Basel Committee on Banking Supervision (the global banking standards setter).[10] They ask banks to provide data to help the Basel Committee and local regulators develop prudential standards that ensure the safety and soundness of banks. Aggregated results are publicly released.

Regulatory requests

41. ANZ also responds to other requests from regulators and authorities for data to assist them with their regulatory functions. An example of this would be requests from ASIC to provide it with detailed information on our operations. Similarly, we provide information relevant to preventing financial crime to the appropriate authorities as required.

Derivatives reporting

42. Under Part 7.5A of the Corporations Act and cognate provisions in other jurisdictions (including the United States and through Asia), ANZ reports data concerning its OTC derivatives to trade repositories that are licensed by relevant regulatory authorities.[11] This data can then be accessed by those authorities and other government agencies. Reporting this highly confidential data helps the official sector understand exposures within the derivatives market.

[8] http://apra.gov.au/adi/Documents/150714-APS-330-August-2015-final.pdf
[9] http://www.shareholder.anz.com/pages/regulatory-disclosure
[10] https://www.bis.org/bcbs/qis/
[11] ASIC's reporting regime is described here: http://www.asic.gov.au/regulatory-resources/markets/otc-derivatives-reform/derivative-transaction-reporting/

Response to Inquiry Questions

Introduction

43. The Commission has posed various questions concerning whether and how the availability of private sector data could be increased and consumers' access to and control over data improved.[12] Rather than responding to each question seriatim, we have collapsed the questions into four areas of discussion.

44. These areas are:

- Is reform needed to liberalise data within financial services?
- If the Commission is minded to recommend reform, what are the distinct legitimate interests in data that need to be recognised in a modern digital economy?
- Given that recognising these interests requires data to be both protected and shared, what policy principles could achieve both objectives?
- What reforms could be pursued to best implement these policy principles?

Is reform needed?

45. As set out above under 'Data in Banking', banks like ANZ already make substantial amounts of data available to their customers, the market and the official sector.

46. The amount of data made available will only increase as:

- Use and availability of data is demanded by digitally-engaged customers
- Product and service attribute disclosure is digitised (as noted above)
- CCR becomes more widespread due to existing investment commitments (again, as noted above)
- Technology advances to make better use of already available data

47. The increased availability of data through CCR will occur as credit providers complete implementing complex system and control development changes. The shift from negative to positive reporting has required substantial resources to ensure that the data reported and collected is well-protected and capable of being used. We are of the opinion that further regulatory reform should not be pursued until this current slate of investment has had an opportunity to deliver change.

[12] Productivity Commission *Data Availability and Use – Productivity Commission Issues Paper* (April 2016), 18, 21.

48. Further and looking ahead, rapidly advancing technology could solve the policy problem that ostensibly invites reform concerning the availability of standardised data.

49. The main argument posited for standardised availability is that data needs to be presented in a standardised format to permit its easy use. Only then would third parties be able to use and manipulate the data.

50. However, much of the banking-related data that could be mandated to be available (eg transaction data and product details) are already accessible to customers in the form of online and digital access to accounts, statements, online transaction histories and via the Privacy Act. Further, product and service attribute disclosure is increasingly being digitised.

51. In this context, it is highly likely that technologies and commercial approaches will develop that can utilise this available data without it needing to be 'standardised'. Artificial intelligence could conceivably 'read' already available data and convert it to a usable format. Voluntary investment in analytical tools by motivated technology companies could quickly override the policy rationale for mandated availability of standardised data. Conversely, mandating standardised data formats risks retarding innovation in data generation, processing and formatting.

52. Combining these points, we would argue that the case for reforming legislative settings concerning the availability of private sector data is yet to be made out. Our strong preference would be that the Commission adopt a wait-and-see approach to private sector data availability before recommending reform.

Interests in data

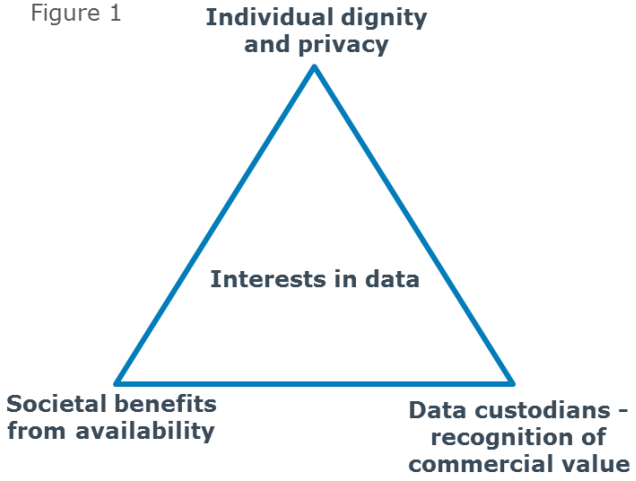
53. If, despite the already widespread and increasing availability of data, the Commission is minded to recommend reform, we believe that there are three key interests in data that the Commission should consider in developing its recommendations:

- The interests of individuals in protecting their privacy and dignity with respect to data concerning them that private sector actors hold.
- The commercial interests of those who generate, organise, secure, analyse and make available data (termed **data custodians**) to protect and profit from the value of their investment in such activities and the derivative value of the data that they hold.

- The benefits to society that could accrue from greater availability of private sector data.

54. These interests can be depicted diagrammatically as follows:

Figure 1



55. Unless all three interests are appropriately recognised and aligned through policy settings, it is possible data will not be generated, used and made available as efficiently and effectively as possible.

Privacy and dignity

56. The interests of individuals in having their privacy and dignity protected with respect to data underpin the Privacy Act.[13] The Privacy Act empowers the Office of the Australian Information Commissioner to enforce minimum standards governing third party treatment of data concerning individuals.

57. The protections of the Privacy Act help individuals trust that third parties with whom individuals share personal data will respect that data. The importance of this trust to the viability of modern commercial enterprises that are built on data and the corresponding availability of such data for societal benefit cannot be understated. Without that trust, data availability would diminish.

Commercial value

58. In a digital economy, data can be exceptionally valuable. This value derives from its ability to deliver insights and underpin services and products.[14] Further, the creation, collection, organisation and storage of data involve cost. Data

[13] See Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (2008), 104 stating that '[a]s a recognised human right, privacy protection generally should take precedence over a range of other countervailing interests, such as cost and convenience.'

[14] For a discussion concerning the value of personal data in the economy, please see World Economic Forum *Personal Data: The Emergence of a New Asset Class* (2011); available at: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

custodians willingly incur these costs because of the commercial value provided by data.

59. Data custodians would be legitimately concerned from a commercial and equity perspective if policy settings concerning data did not recognise this 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.

60. For this reason, we would argue that the commercial value of private sector data needs to be recognised in order to ensure data's public benefits are fully realised. Allowing data custodians to exclude others from, and then conditionally permit access to, their investment is necessary to incentivise data generation. While data custodians will always have reasons to invest in data generation, these reasons will be diminished if the benefit from the investment can be captured by others without reward to the data custodian. This negative externality would potentially diminish the volume and quality of data that is available to society.

Societal benefits from availability

61. Society could benefit from increased data availability. For example, data reporting under Part 7.5A of the Corporations Act helps the official sector monitor and respond to positions within the OTC derivative market.

62. Further, initiatives in the United Kingdom and the European Union to make more customer data available are predicated on the basis that data could be used to help customers make better purchasing decisions.[15] Failure to appropriately use data for societal benefits could undermine growth, productivity and customer engagement. We strongly support better customer engagement.

63. As the Commission assesses the potential societal benefit from data availability, we would encourage it to take an evidence-based (rather than a hypothesis-based) approach to identifying those policy measures which could improve customer engagement and thus deliver societal benefits.[16]

---

[15] See the UK midata initiative: https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment. For the relevant European Union provision, see Article 20 of *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*

[16] For example, see Jigsaw Research *Potential consumer demand for midata Findings of qualitative and quantitative research*; available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34742/12-976-potential-consumer-demand-for-midata.pdf . This report identifies at 3 that

When initially shown an expression of the midata concept, consumers were bewildered about why this is being proposed and what difference it would make. As consumers typically define personal data as personal identity

Value in data

64. Each of these three interests could derive utility from different and overlapping data sets depending on their intent and position. For example, society could benefit from individuals in aggregate having access to data concerning their transaction histories to understand their historical financial behaviour. Data custodians could similarly benefit from this data but also from data which has been subject to substantially more analysis and change (thus benefiting the consumer).

65. While it is difficult to posit in abstract the value individuals and entities could derive from data, and recognising that are no doubt multiple ways to conceptualise value, we would propose a value heuristic based on two dimensions:

- The degree of granularity of the data.
- The level of investment, change or analysis that has been applied to it.

66. For example, basic data concerning an individual (eg name, address) may be of less value to them, while more detailed data concerning, for example, their transactions may be of more value. Similarly, data to which a data custodian has applied minimal investment in changing or analysing may be of less value than data that has been subject to substantial analysis and rearrangement.

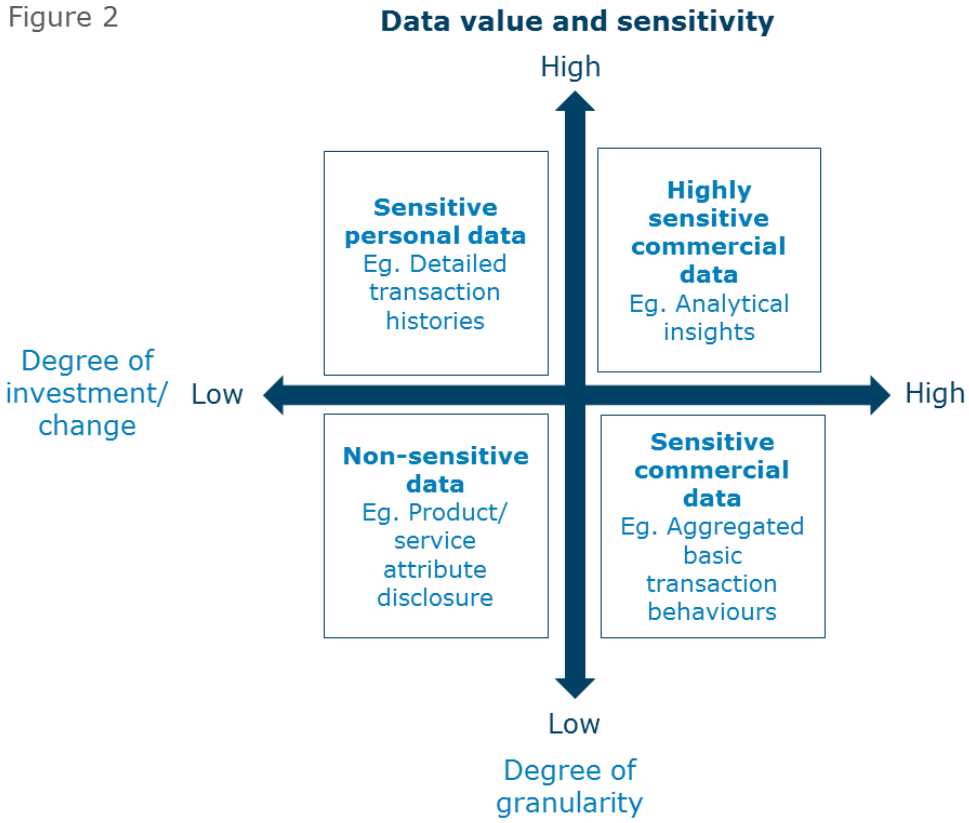
---

information, they struggled initially to identify what benefits the release of such data (which they already own/know) would have for them.

This bewilderment was only overcome once use cases were demonstrated to consumers. This implies that there are substantial educational hurdles to be overcome in engaging consumers in the ostensible benefits derivable from greater data availability.

67. Figure 2 sets out how this value heuristic could be conceptualised.

Figure 2



68. Using this heuristic may help the Commission identify those data sets which present more or less value to various interests.

69. From our perspective, we see substantial value in data sets which are either more granular or have been subjected to investment or analysis. We would see these data sets as deserving of particular protection from a data custodian's perspective. Examples of such data sets could be those that have been subjected to proprietary algorithms. Indeed, these data sets could be the subject of so much investment and provide so much commercial benefit that they would never be suitable for release.

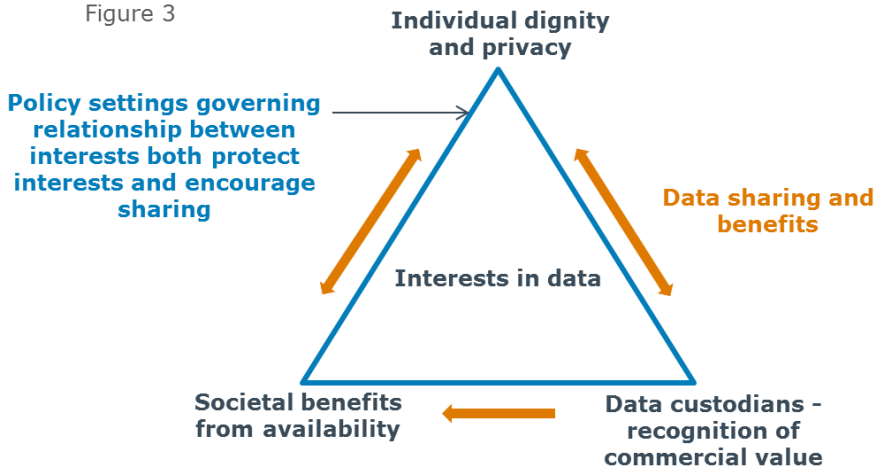
Promoting and balancing the interests

Introduction

70. Each of the three interests we have identified is important. As such, all three need to be appropriately recognised. However, recognition of all three interests involves both protecting data held by data custodians or pertaining to individuals and simultaneously promoting the sharing of that data. This raises a potential conflict between protection and access.

71. A possible end-state is set out in Figure 3.

Figure 3



72. The policy challenge is then to find the right settings that resolve this conflict. We think that the Commission faces a choice between the following settings:

    a. Public ordering through mandating the availability of data;[17] and

    b. Private ordering through encouraging data custodians and individuals to voluntarily make data available, through either:

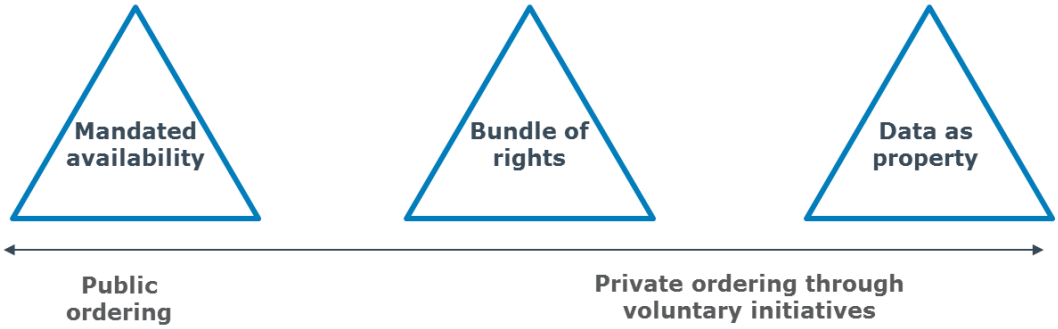
        i. The bundle of rights that attach to data; or

        ii. Making data personal property (ie beyond copyright).

[17] By public ordering, we mean initiatives by the state to mandate that specified entities should make specified data available. For example, see the powers in section 89 of the United Kingdom's *Enterprise and Regulatory Reform Act 2013*. These powers allow the 'Secretary of State' to require a regulated person to provide customer data to either the customer or their agent.

73. These policy setting options can be set out visually as follows.

Figure 4 **Continuum of potential policy settings**



74. In our opinion, the most apt policy setting is private ordering through a well-calibrated bundle of rights. We believe that this setting would allow all three interests to be recognised equally. Such equal recognition would encourage the sharing of data for social benefit.

Why mandated availability does not recognise all three interests equally

75. Before explaining how a well-calibrated bundle of rights could align all three interests, it is worth setting out our thoughts on why mandated availability of data would fail to achieve such a balance. There are two key issues that we believe the Commission should consider.

Security of data and privacy

76. The first key issue is that it is possible that mandated availability of data could undermine individual privacy and dignity through impaired data security. Impaired data security could decrease the amount of trust that individuals have in sharing their personal data, negatively impacting data availability. This concern has four drivers.

77. **First**, it is conceivable that mandated availability could be achieved by requiring data custodians to allow third parties access to customer data if that customer authorised the third party. In this case, the third party would presumably be entitled to obtain and use customer access details (for example PINs, usernames and passwords).

78. Once third parties hold customer access details, then customers are exposed not only to fraud and misuse by and within those third parties but also the theft of those details by other parties (eg through hacking). Banks have sophisticated means of preventing unauthorised access to customer accounts. However, these

means may not be able to prevent access by malicious third parties who have acquired customer access details.

79. Further, data custodians would be legitimately concerned about who bears liability for losses that may arise from 'authorised' but fraudulent access. For example, is it the customer, the third party who was given the customer access details or the data custodian who should bear the losses for such breaches?

80. We note that, under the E-Payments Code, users of electronic payment services are required to not disclose access details to third parties. This requirement is to ensure that the integrity of their payment service is not compromised. For similar reasons, non-disclosure of access details is also a condition of the contract between many banks and customers.

81. **Second**, adopting and implementing security measures that are resistant to contemporary hacking attacks requires substantial resources. The Australian Government states that '[a]lmost one million Australians were estimated to be victims of identity theft online in 2014'.[18] Critically, mandated availability of data could see sensitive personal data held by entities without the capabilities to properly protect it. Increased data availability also raises the concern of social engineering attacks. As more data is available for misappropriation, it would become easier for identities to be stolen and assumed by criminals.

82. Of course, these concerns apply to all situations where data is more available. Accordingly, as data availability increases, we would encourage the Commission to consider the imperative that current regulatory requirements to secure data are applied universally.

83. **Third**, we would be concerned that third parties could obtain permission to access customer accounts with less transparency than is necessary to ensure customers are fully aware of the implications of granting permission. For example, customers may be defaulted into providing access as part of a sign-up process for a service which is ostensibly only tangentially related to access.

84. In this vein, data custodians would likely be obliged to or, indeed, wish to verify that individuals had provided consent to access. This would place a substantial administrative burden on data custodians.

85. **Fourth**, releasing increasing amounts of data increases the ability to combine disparate data sets to identify individuals or commercial positions. For example,

[18] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy*, 16.

released data could be cross-referenced against an already available data set in a way that identifies individuals or their situations. The Commission will need to consider how to ensure that interests of individuals and data custodians are not compromised by the release of data for apparently limited purposes enlivening other data sets. Again, this concern applies to all situations where more data is available.

Undermining of commercial interests

86. The second key concern is that mandated availability could undermine the legitimate interest which data custodians have in the investment they have made in establishing and maintaining data sets. Undermining this interest could have two ramifications.

87. **First**, as discussed above, mandated availability would undermine incentives for data custodians to invest in data generation, organisation and protection. This would have negative consequences for the availability of data in society.

88. **Second**, mandated availability could generate imbalances and inequities between competing commercial interests beyond the negative externality highlighted above.

89. For example, if sufficient customers of a bank all make their data available to the same commercial enterprise, such as a comparison service, that enterprise would hold a meaningful replication of that bank's customer data and thus a strong understanding of the bank's commercial position. This understanding could either be valuable to the enterprise if it ultimately wished to offer products and services in competition to the bank or to the bank's competitors, if the enterprise were able to sell the data. If data availability were to be mandated then, as set out above, we would be concerned that data custodians may decrease their investment in data integrity and collection.

90. Of course, we are not contending that mandated availability would cause data custodians to stop collecting and protecting data. Such entities will have endogenous reasons for performing these activities, including better servicing their customers. However, mandated availability could chill this behaviour, diminishing it below levels that would otherwise obtain.

Other issues with mandated data availability

91. In addition to the issues that mandated data availability poses to legitimate interests in data, we believe that it could pose two additional issues that the Commission would benefit from considering.

Cost of availability

92. Increasing the availability of data would impose costs on current data custodians, particularly if the format of the data availability were prescribed. The cost of increased availability would vary with the quantum of data made available and the nature of its availability.

93. Banking information systems have developed over time with a variety of architectures. Developing standardised data structures is time consuming and resource intensive. Where data is exchanged, for example CCR, considerable effort is made in developing data architectures that can transform data into a common readable format.

94. As noted above, we estimate that industry costs in developing the infrastructure necessary to deliver CCR will cost approximately between $400 and $500m. We would expect similar costs, if not more, to accompany initiatives to require availability of a broader data set on a standardised basis. Such a quantum of cost would require significant quantifiable benefit to be justifiable (refer to our comments at paragraph 63 above).

Standards

95. Lastly, the technical standards through which data was made available would need to be carefully considered and acceptable to current data custodians. Such businesses would be legitimately concerned if standards were imposed on them without the ability to participate in their development and specification. Similarly, there would need to be agreement concerning the definition of data and how it was to be delivered.

96. We note that the Australian Credit Reporting Data Standard that underpins CCR was developed by the Australian Retail Credit Association, an industry body. This is a useful example of industry-led development.

97. Similarly, we think that the Commission may find utility in considering the CCR experience with respect to dispute resolution. As data becomes more important and available, its accuracy will also become more important. Ensuring that customers have adequate redress avenues for data errors would be a critical element of an environment where data is more widely available.

Voluntary data sharing

98. While we do not believe that mandatory data sharing can align the three interests in data, we do think that policy settings that encourage voluntary data sharing could. Such settings could bring the three interests into mutually supporting alignment.

99. Thus, 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 data can be made available, then societal benefits could result.

100. In such an environment of mutual alignment, we would expect that competitive forces would drive greater data availability and use.

- To the extent that customers demand data in this environment, then data custodians would likely feel comfortable providing it.
- Similarly, to the extent that innovative service providers identify high-value uses for data, then they are likely to find data available from enterprising data custodians (subject to the Privacy Act).
- Further, voluntary data sharing could be established on the basis of reciprocity under which data custodians make data sets available in exchange for access to the data sets of other data custodians.

101. To achieve this mutual alignment of interests, we believe that:

- Individuals need to be able to control who has access to their data and on what terms; and
- Data custodians need to be able to establish and licence exclusive rights to their databases that they maintain and the outputs from such databases.

102. Both of these states could be achieved theoretically through two legal mechanisms:

- Recognising data as property; and
- Attaching a set of rights to data that protect individuals' interests in personal data and data custodians' investment in data generation and protection.

103. Which, then, of these two mechanisms is superior in aligning interests?

104. Under current Australian law, it appears that data is best characterised as being subject to a bundle of rights and not as property.[19] For example, the High Court in *Breen v Williams* has recognised that 'information' (in the context of information in medical records) is not property.[20]

105. Instead, there are a bundle of rights concerning data's use, protection and access.[21] These rights include:

- **Privacy Act** – Individuals have overriding rights to access and correct personal data concerning them.
- **Copyright** – Data which has been captured in a literary work subject to copyright, such as a table or compilation, benefits from protections under the Copyright Act. However, recent jurisprudence concerning databases indicates that copyright protection for elements of databases, particularly those compiled mechanistically, may be weak. We discuss these limitations below.
- **Breach of confidence** – Unauthorised use of confidential data which is shared with another under certain conditions could give rise to an action for breach of confidence.
- **Bankers' duty of confidentiality** – Bankers have a duty to hold information concerning their customers in confidence.
- **Contractual rights** – A contract could establish rights between the contracting parties concerning data. However, such rights would not be enforceable against third parties.

106. In considering whether law reform should pursue the propertization of data (particularly for individuals), we would argue that property rights would be less effective than a bundle of rights in aligning the interests.[22] This is because:

---

[19] See Leif Gamertsfelder *Corporate Information and the Law* (2nd ed, 2016, Butterworths), 13. Gamertsfelder identifies that '…the High Court of Australia has repeatedly rejected the proposition that information per se is proprietary in nature'.

[20] *Breen v Williams* (1996) 186 CLR 71; see statement of Dawson and Toohey JJ that there 'can be no proprietorship in information as information'. Judgment available at: http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/cth/HCA/1996/57.html?stem=0&synonyms=0&query=title(breen%20and%20williams%20)

[21] See Gamertsfelder, above n 19, chapters 2, 3 and 4 for a discussion of these types of rights (with the exception of the bankers' duty of confidentiality). In saying that data is subject to a bundle of rights, we recognise that property law in general can similarly be said to be constituted by a bundle of rights. We use the term here to refer to a collection of rights that fall short of a proprietary interest in data as a thing.

[22] In considering the issues concerning the propertization of data, we would refer the Commission to the work of the American Bar Association's Section of Science & Technology Law: Data Property Rights Committee. This committee has produced a literature summary on data property rights, with a focus on the law of the United

- Applying property right concepts to data is problematic for the reasons given in *Breen*, namely, that data cannot be alienated like traditional personal property (ie two or more people could simultaneously possess the same proprietary interest in data).
- While property rights could perform the same function as the protections under the Privacy Act, this would require individuals (rather than a central agency) to enforce those rights and protections.
- Rights under the Privacy Act cannot be surrendered while proprietary interests in data could. It is conceivable that private sector entities could require the surrender of proprietary rights in personal data as the price of services.
- Full property rights would pose a high hurdle to effective data sharing.

107. In contrast, a bundle of rights could be crafted that allows all interests to be recognised and balanced. As such, we would contend that the bundle of rights approach holds promise as the superior policy setting.

Amendments to current rights to encourage data sharing

108. However, simply stating that data should be subject to such a bundle of rights does not resolve the issue of what rights are needed.

109. Existing protections under the Privacy Act appear to sufficiently underpin interests of the individual privacy and security of personal data. We acknowledge that the Commission will consider offshore regimes that provide greater access rights to individuals with respect to data that relates to them. As we have noted, we believe that ensuring individuals trust entities which collect, store and use personal data will be critical in ensuring the success of Australia's digital economy.

110. With that acknowledgement, we would contend that more could be done to support the interests of data custodians with a view to encouraging them to make more data available.

111. As noted above, recent jurisprudence concerning databases means that there are potentially weak rights concerning data within and, critically, derived from databases. Data itself does not appear to be property. Further, there are

States. The summary is publicly available at this link: http://www.americanbar.org/content/dam/aba/administrative/science_technology/2014_data_prop_rights.pdf.authcheckdam.

number of limitations with relying on current copyright law to protect data in databases in Australia.

- **Form of expression** – The only protections in the Copyright Act which are potentially applicable to the type of data under consideration are those extended to literary works and then only to the compilation rather than the raw data *per se*. This means that raw data extracted from a database and re-arranged would unlikely be protected by copyright.[23]
- **Authorship** – It may be difficult to prove that a database compiled by computer program has an 'author' for the purposes of the Copyright Act due to the absence of human involvement and the difficult of evidencing joint authorship.[24] This problem will only become more acute as computer technology advances and human intervention decreases.
- **Substantiality** – Replication of part of a database will only attract copyright protection when the part replicated is 'substantial', assessed both quantitatively and qualitatively. Thus, 'insubstantial' usages of databases will not be protected.

112. These limitations are brought into starker relief when considering the situation of a data custodian that compiles data into a database and then releases that data. Such a data custodian would hold a copyright interest in the database but only retain such an interest to the extent that the data was released in the form of a substantial replication of the database. In particular, where the data was released via some form of application programming interface (**API**) that extracts the data and organises the dataset according to its terms, then it could be difficult for a data custodian to claim authorship. Leaving aside possible limited protections that could be afforded by contractual arrangements, no legal rights or protections would otherwise attach to the data notwithstanding that the original

[23] See Gamertsfelder, above n 19, 36 citing the comments of Upjohn J in *Football League Ltd v Littlewoods Pools Ltd* [1959] 1 Ch 637 that 'scrambling' of information originally contained in a copyrightable list into a new order could mean that the scramblers 'were using only the information and were not reproducing the compilation'.

[24] Gamertsfelder states:
The Full Federal Court's decision in Phone Directories *indicates that in a copyright context the courts will not 'look through' technology to the human actors that designed systems that produce works, especially in the absence of any evidence that compels them to do so. Accordingly without legislative reform the law of copyright will not be able to afford protection for large-scale databases in Australia for two reasons. First,* Phone Directories *demonstrates that it will be incredibly difficult to provide the required evidence of human authorship where technology performs the final 'transformative step' in that production of a work. Second, even if evidence of some human authorship was produced and accepted, it would be difficult to demonstrate that such authorship so as to satisfy the joint authorship requirement in the Act.* Gamertsfelder, above n 19, 48.

organisation of the data which allowed its release was undertaken by the data custodian.

113. This situation is set out in Figure 5.

Figure 5

Current Protection of Data in Databases

Transformative process	Raw data	Captured in corporate database	Released as either subset of database, API dataset or raw data
Data state	1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0 →	Database →	1 → Database subset 2 → API dataset 3 → 1, 0, 0, 1,
Current legal treatment	Probably not property	Bundle of rights including copyright and Privacy Act	1 Database subset –level of protection based on *Copyright Act* depends on authorship and substantiality 2 API dataset – Query who has copyright in dataset as 'author' is API program 3 Raw data – no protection (maybe breach of confidence)

114. The effect of this is that data custodians may not be able to control the terms on which data are used once released. As noted above at paragraphs 86-90, such usage could involve commercial activities detrimental to the data custodian's interests. Concern about this could limit the extent to which data custodians invest in data generation, protection and availability.

A new sui generis *right in databases and their outputs*

115. To counter this, we would suggest that the Commission consider recommending that Government legislate for a new *sui generis* right in databases and their outputs that could vest in data custodians.[25] This right would allow data custodians to protect their interests in data and allow them to provide access to databases confident that those interests will be protected.

116. Precedent for creating this new right lies in the European Union's *Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the*

[25] We make this recommendation cognisant that the Commission is currently inclined of the view that no major reforms are needed to the originality concept in Australian copyright law; Productivity Commission *Intellectual Property Arrangements, Draft Report* (April 2016), 105.

Legal Protection of Databases (**Database Directive**). Article 7 of the Database Directive requires that

> *Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.*

117. Recommending that Australia should have protections similar with those afforded by the Database Directive would accord with curial comments concerning the ability of Database Directive protections to fill a lacuna in the protections afforded by the Copyright Act.[26]

118. We believe that a modern Australian database right should have the following attributes:

- Protection would apply to the investment in creating and maintaining databases, broadly understood and regardless of whether the data custodian created or collected the data housed in the database.[27]
- The right would allow data custodians to permit third parties to obtain and use data that is drawn from a database under licence, regardless of the form of expression of the data.
- The right would be good against the world, not merely third parties authorised by licence to obtain and use the data.
- It would not override rights originating in the Privacy Act. The protections afforded by that Act would be undiminished. As such, both individuals and data custodians would simultaneously hold rights over data, with individuals' rights under the Privacy Act dominating.
- As in the case of the Database Directive, the right would be additive to existing copyright protections.

---

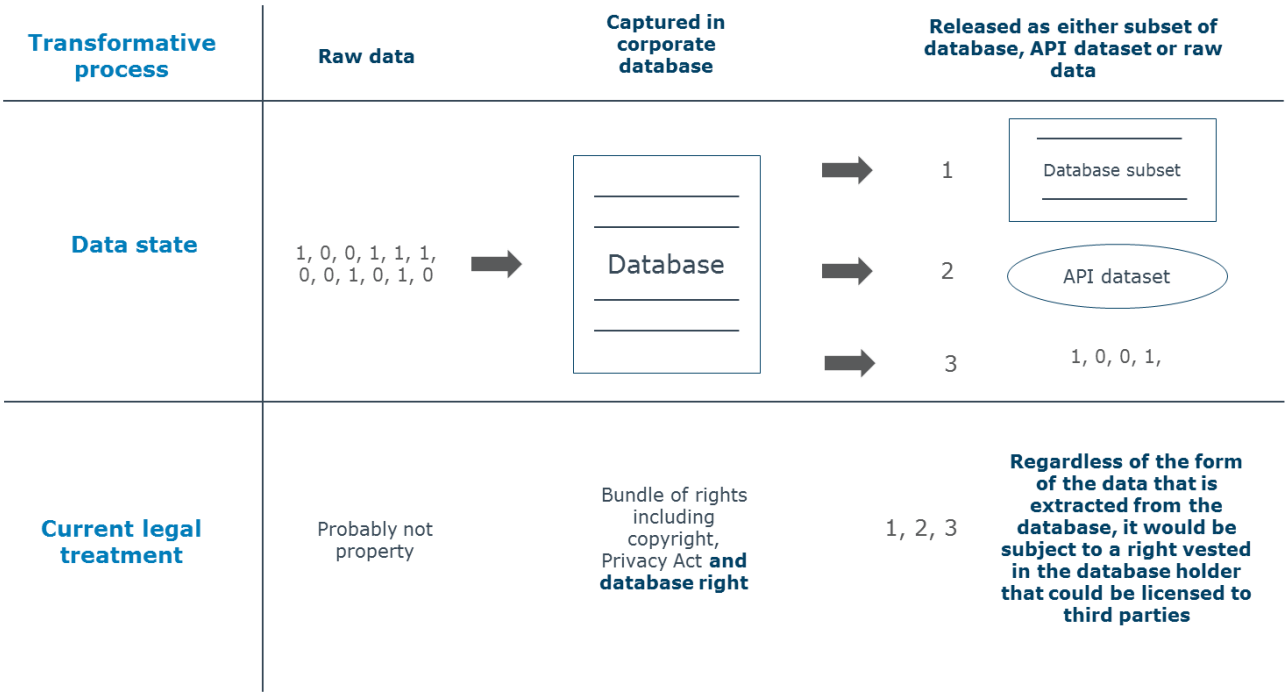
[26] The idea of introducing a right similar to that created by the Database Directive has been suggested judicially. Justice Gordon in *Telstra Corporation Ltd vs Phone Directories Company Pty Ltd* [2010] FCA 44 at 40 stated that the expansion of protections consistent with the Database Directive is '…a matter which [Parliament] should address without delay'. See discussion in Gamertsfelder, above n 19, 49.

[27] Article 7 of the Database Directive has been interpreted to remove the right where data has been 'created' by the database holder; see *British Horseracing Board Ltd and others v William Hill Organization Ltd* of Case C-203/02, [2004] ECR I-10461. The implication of this interpretation is that data which is created within an organisation may not be protected whereas data which is collected or obtained from sources external to the organisation would be protected. Such a result obviously diminishes the utility of the right severely. See the discussion in Gamertsfelder, above n 19, 63.

- The right would not represent a property interest in data per se. Rather, the right would be grounded in the investment by the data custodian in a database and extend to the product of that investment, including when data was extracted from the database.

119. Figure 6 sets out the result of creating such a right in the scenario depicted by Figure 5.

Figure 6 **Protection of Data in Databases using Proposed Database Right**



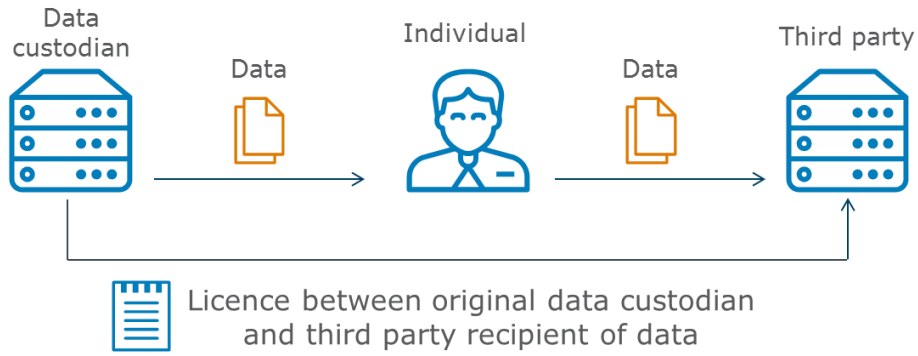
120. Vesting such a right in data custodians would encourage data availability by allowing custodians to benefit from investing in data and its availability. Data custodians would be able to more confidently licence third parties to use data that is collected by the custodian. In this sense, it would more completely align the interests of data custodians with the objective of making more data available than mandated availability could.

121. Further, such a database right would not undermine the interests of individuals. Individuals would still be able to exercise the rights granted by the Privacy Act as those rights would be superior to the database right. This would allow them to have a say on the terms on which database custodians use data which relates to their personal details.

122. If individuals were granted a right to access and port data concerning them, then such right would operate in tandem with the database right. This would mean that individuals could download their data and pass it on to a third party who held

a licence from the original data custodian to use the data. A diagram of how this could work is in Figure 7. The licence could allow for direct routing of the data from the data custodian to the third party when authorised by the individual.

Figure 7 **How data could be shared using database right**



123. However, even in the situation where data custodians could license use of data extracted from their databases, we note that there are likely to be data sets that data custodians would legitimately never wish to make more available. Such data sets may be those which have been subjected to substantial investment or which provide legitimate competitive advantages. In this regard, see paragraph 69 above.

124. The Commission may like to consider if an industry protocol could be established that may be acceded to by data custodians and third parties to save multiple bilateral negotiations. In this vein, an industry protocol could establish measures design to protect the cyber-security of shared data. For example, closed user groups organised around a central data bureau could provide means of access, sharing and security.

125. Additionally, such a database right would not undermine CCR. Data custodians would simply contribute their credit reporting data to credit bureaus on the basis of a licence that allows the use of the data for the purposes of reciprocal CCR and credit worthiness assessment.

126. If such a right were added to the protections already provided by the Privacy Act, then we believe that Australia would have a well-calibrated bundle of rights concerning data. This would help align the three interests in data.

ENDS