University of New South Wales Law Research Series

JOINT SUBMISSION TO TREASURY ON THE OPEN BANKING REVIEW FINAL REPORT

KATHARINE KEMP AND DAVID VAILE

(2018) Submission to Treasury, *Final Report of the Review into Open Banking in Australia*, 9 February 2018

[2018] *UNSWLRS* 23

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications

OPEN BANKING REVIEW

Final Report

Submission to Treasury

Katharine Kemp and David Vaile*

23 March 2018

Introduction

1. This submission responds to the Final Report of the Review into Open Banking in Australia released by Treasury on 9 February 2018 ('Final Report'). It makes a brief summary of the broader significance of the Open Data regime advocated by the Productivity Commission in its Report on Data Availability and Use,[1] followed by responses to some specific recommendations of the Final Report.

The Fundamental Effect of Open Data on the Landscape of Power in Australia

2. It is no exaggeration to say that the push for 'Open Data' – and 'Open Banking' as its first incarnation – is likely to fundamentally affect the balance of power in Australia between firms and consumers, between data subjects and data controllers, and between government and citizens, for generations. The balance, and much of the benefit, is weighted towards firms, data controllers and governments, and away from citizens. It is therefore critical that the risks are properly assessed and appropriate protections or restrictions are developed, tested and put in place before any decision is made to implement such a radically different regime to that which is in place at present.

* Katharine Kemp, Lecturer and "Data as a Source of Market Power" Research Stream Co-leader, UNSW Law Faculty, Allens Hub for Technology, Law and Innovation; David Vaile, "Data Protection" Research Stream Leader, UNSW Law Faculty, Allens Hub for Technology, Law and Innovation.

[1] Productivity Commission, Australian Government, 'Data Availability and Use' (Inquiry Report No 82, 31 March 2017) ('Productivity Commission Report').

3. One of the aims of the 'Open Data' regime is to greatly increase the amount of personal information which is collected, processed and disclosed in Australia. It is important to appreciate that Australia's existing data protection regime is fundamentally deficient. Data subjects in Australia have no capacity to go to court to enforce the law in the event of a breach or an abuse. There is also a wide range of exceptions for business and government in the existing law, some of which are excessive and hostile to data subjects, and an over-reliance on often poorly informed 'consent' mechanisms, which compromise the interests of the unsophisticated. Critically, Australian privacy law lacks any right to sue for intrusion of privacy, in contrast to the privacy laws in most comparable countries, notwithstanding the recommendation of a statutory cause of action for serious intrusion of privacy by the Australian Law Reform Commission (ALRC) in 2014.

4. Without improved legal protections, the proposed dramatic increase in collection and disclosure of personal information will operate to the detriment of consumers by exposing them to proportionately greater risks from the unauthorised and fraudulent use of their personal information, from the aggregation and discriminatory use of their information, from ever greater risks of data breach due to the continued erosion of IT perimeter security and expansion in intruder capacity, and from other new potential misuses that will arise from the rapidly expanding capabilities of 'Big Data' and artificial intelligence technologies and the proliferation of other data sets,[2] and the proliferation of data sets 'in the wild' from all sources, legitimate and compromised.

5. In its report in support of the Open Data regime, the Productivity Commission recommended that to achieve the necessary 'social licence' for this increased disclosure of personal information the government should enact a 'Consumer Data Right' that would provide consumers with certain rights in respect of their personal

[2] Eg, in the recent Cambridge Analytica breach case.

information,[3] some of which consumers already possess under existing privacy legislation.

6. The stated goal of this 'Consumer Data Right' is that consumers should be empowered.[4] This goal will not be achieved if the net effect of the Open Data regime is that a much larger amount of consumers' personal information is collected, processed and shared in a way that exacerbates inequalities in bargaining power, information asymmetries, discriminatory treatment and exclusion of vulnerable groups, especially if their existing exposure to risk without an effective remedy is not addressed. If this is the result, consumers will have relinquished what is left of their private domain and commercial agency for a trinket.

Regulatory Approach: Competition and Consumer Act – Recommendation 2.1

7. This submission supports the recommendation that, if Open Banking is implemented, it should be implemented primarily through amendments to the *Competition and Consumer Act 2010* (Cth) ('CCA') that set out the overarching objectives of the Consumer Data Right (Recommendation 2.1).

8. Situating the Consumer Data Right in the CCA is consistent with the respective objectives and scope of the Consumer Data Right and the CCA, and acknowledges that competition cannot be optimised without adequate consumer protection and vice versa.[5]

9. It is proposed that the Consumer Data Right, like the CCA, will ultimately be implemented on an economy-wide basis. The Final Report refers to four principles for Open Banking, namely that it should, to paraphrase:

[3] Productivity Commission Report, above n 1, 13-15.

[4] Productivity Commission Report, above n 1, 177-180.

[5] See Geraint G Howells and Stephen Weatherill, *Consumer Protection Law* (Dartmouth, 1995) 142-144; Organisation for Economic Co-operation & Development, *Consumer Policy Toolkit* (2010) 31-33 ('OECD Consumer Policy'.

- be customer-focused and implemented for the benefit of customers;
- encourage competition to enable better customer choices;
- create opportunities for new ideas and businesses to emerge and grow; and
- be efficient and fair, having particular regard to security and privacy.[6]

These aims are consistent with the overarching object of the CCA, which is:

> to enhance the welfare of Australians through the promotion of competition and fair trading and provision for consumer protection.[7]

10. **The symbiotic nature of competition and consumer protection is part of the fabric of the CCA. The scheme of the act recognises that consumer protection is essential to well-functioning competition.** Effective competition depends on consumers having access to accurate information and the ability to bargain for, and switch to, a better deal. Further, while the CCA promotes competition, case law under the statute has established that a mere increase in the number of rivals in a market does not necessarily mean that competition is improved. Effective competition is competition which drives superior efficiency and innovation and is responsive to consumers.

11. The Consumer Data Right is intended to create numerous benefits for competition and consumers, including reduced switching costs; reduced barriers to entry for new providers, leading to increased consumer choice; and reduced inequalities in bargaining power. The effects of 'Open Data' on competition have not yet been tested and established.[8] However, the desired benefits are all central concepts under the CCA, which also provides mechanisms for testing the health of competition in specific markets, including by way of market studies.

---

[6] Final Report, v.

[7] *Competition and Consumer Act 2010* (Cth) ('CCA'), s 2.

[8] Nor have the risks, which are potentially diffuse and difficult to detect or remedy: see 'Report of the Special Rapporteur of the Human Rights Council on the Right to Privacy' (A/72/43103, Advance Unedited Version, 19 October 2017) 7.

Regulatory Responsibility: Competition and Privacy Overlap – Recommendation 2.2

12. This submission supports the recommendation that, if Open Banking is implemented, it should be supported by a multiple regulator model, led by the Australian Competition and Consumer Commission (ACCC), which should be primarily responsible for competition and consumer issues and standards-setting (Recommendation 2.2), but makes a qualification concerning the need to avoid neglecting privacy protection or divorcing it from these issues.

13. The ACCC is a highly-regarded regulator with economy-wide powers and over 40 years' experience implementing the competition and consumer objectives of the CCA. It is therefore well-equipped to implement the objectives of the Consumer Data Right. It is also sensible that the ACCC should work with the Office of the Australian Information Commissioner (OAIC), given its role and experience in enforcing the *Privacy Act*.

14. However, it is submitted that **further debate is required about how responsibility for competition, consumer and privacy issues, as well as investigative, representative and enforcement powers, should be divided between these regulators**. Critical issues and incidents under the Open Data regime are likely to involve an overlap between these areas and will require a cohesive and certain regulatory response.

15. Effective competition is driven by consumers shifting their spending to those firms that best satisfy their needs and wants. Rival firms are thereby compelled to innovate and improve their efficiency or risk losing business. This driving force cannot function optimally when there are gross information asymmetries: for instance, where consumers possess vastly inferior information about the proposed transaction relative to suppliers.

16. Open Data may aid firms in exacerbating such information asymmetries, allowing them to compile extensive, aggregated information about consumers and create an all-seeing, all-knowing "god view" of the individual,[9] which cannot be viewed by the consumer in question. Consumers may be given a window of light on some of their personal data while firms use profiling, microtargeting and manipulation to take advantage of consumer needs, habits and vulnerabilities.[10] These firms would not be using data to increase their efficiency, aid innovation or enhance competition, but only taking advantage of greater information asymmetries to better exploit consumers. That is, **failure to protect consumer privacy can substantially degrade competition in a market.**

17. The recent exposure of abuses of profiling by Facebook demonstrate both the global scope and import of such abuse, and the weak position of consumers when it occurs at present (even more so when they are in Australia and the data is in another jurisdiction, since Australia has not insisted on the equivalent of the US *Judicial Redress Act* of 2015, negotiated as part of the new Privacy Shield with the EU).

18. Research to date shows that markets do not tend to self-correct for these deficiencies, in large part because consumers are unaware of the data practices or the resulting prejudice to their bargaining position.[11] Such uses of personal information raise competition and consumer issues, including increased inequality in bargaining power,[12] increased information asymmetries, unconscionable conduct, and misleading and deceptive conduct. It is by no means clear that resolving such problems should be the preserve of the OAIC with its relatively limited existing powers under the *Privacy Act*.

---

[9] Ariel Ezrachi and Maurice E Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press, 2016) 72-75.

[10] European Data Protection Supervisor, 'EDPS Opinion on Online Manipulation and Personal Data' (Opinion 3/2018, 19 March 2018) 8-9.

[11] Maurice E Stucke and Allen P Grunes, *Big Data and Competition Policy* (Oxford University Press, 2016) 51-57.

[12] As the vendor knows ever more about the consumer, and the consumer is ever less certain about the capacities and links of the vendors.

19. However, a strengthened privacy regime, which takes into account the risks of Open Data, and a capacity for individuals or classes to take their own legal action, is a necessary starting point. In the same way as there are litigation options under consumer legislation, this scheme needs as a condition prior the passage of a general privacy tort with capacity to address the future complex risks arising from schemes of weakly protected disclosure of personal information such as Open Data.

Open Banking Rules: Context, Rule-making and Error Costs – Recommendation 2.4

20. This submission supports the recommendation that the ACCC, in consultation with the OAIC, and other relevant regulators, should be responsible for determining Rules for Open Banking and the Consumer Data Right (Recommendation 2.4), but makes qualifications concerning the significance, timing and substance of this rule-making, particularly having regard to likely error costs.

21. As to the significance of the rule-making, it is important to place Open Banking in its context. Given that banking is to be the first sector designated under the Open Data regime, the rules made for Open Banking should not only take into account the need for consistency between sectors but also **the economy-wide impact these rules will have as a precedent**. That is, regulatory missteps in these rules are likely to be perpetuated.

22. The rule-making should accordingly take place in **consultation** with relevant stakeholders prior to the more technical standard-setting by the Data Standards Body, which is to add detail to the norms and principles established by the rules. With regard to **timing**, while these two processes may overlap in time, the rule-making should take the lead if the proposed hierarchy of regulation is intended to be meaningful. As noted earlier, a condition for the commencement of this regime should be the prior passage of the tort of serious intrusion of privacy, with specific accommodation for new types of Open Data risks. This should be in place prior to the rule making and standard setting, in order to ensure consistency and compatibility of regulatory approaches.

23. Further, it is submitted that **the initial rule-making should take into account the relative error costs of overly permissive and overly protective rules in this context. It will be near impossible to undo the damage done to consumers if the initial rules are overly permissive.** Once a confidential fact is published, it cannot be 'unheard'. Once personal information is collected, disclosed and distributed across various jurisdictions, there is no retrieving it. The horse has bolted. With current technology, that information can be stored indefinitely and aggregated in perpetuity, throughout the lifetime of the individual it concerns.

24. Even more seriously, attempts to de-identify information so that they may be safer to use as Open Data are likely to be constantly undermined by regular advances in Big Data and machine learning techniques for *re-identification*, so that data previously considered 'safe' to release later becomes unsafe.[13] This risk may require long term audits and surveys by sophisticated networks of investigators to identify both failures of previously safe methods of protection, and individual instances of breaching this sort of protection.

25. On the other hand, if the initial rule-making is ultimately determined to be overly protective, desired efficiencies can later be achieved by changes to the legislation or rules. The costs of this kind of error would be reflected in foregone profits and potentially foregone innovations in the interim. However, the effect would not be irrevocable, as in the case of an excessive exposure of personal information. **This weighs in favour of an initial rule-making which deliberately errs on the side of caution.**[14]

[13] Marian-Andrei Rizoiu, Lexing Xie, Tiberio Caetano and Manuel Cebrian, 'Evolution of Privacy Loss in Wikipedia,' WSDM'16, Proceedings of the Ninth ACM International Conference on Web Search and Data Mining, 22–25 February 2016, San Francisco, USA, pp 215-224. <http://dx.doi.org/10.1145/2835776.2835798>

[14] A 'precautionary principle' approach is appropriate where there is compelling evidence of a potentially very serious risk (in this case, for vulnerable individuals, groups, communities or economic settings), there is uncertainty about actual incidence and impact, but it is an irrevocable step: return, once the step is taken, is not feasible.

Compliance and Complaint Handling: Need for Greater Powers – Recommendation 2.10

26. This submission does not support Recommendation 2.10 as a complete recourse mechanism, on the ground that it does not provide adequate redress in the context of the overarching objectives of the Open Data regime.

27. The Final Report rightly acknowledges the increased risks to personal information created by Open Banking, stating:

> If Open Banking achieves its objective of making it easier for customers to share their data, it will be held by more entities than is currently the case. More points of storage will increase the number of potential stages at which data can be compromised – by being hacked or subject to unauthorised access or disclosure. Similarly, transferring data more often increases the possibility of that data being intercepted or inadvertently sent to an unauthorised party, or the wrong data being sent to an authorised party.[15]

28. The Final Report therefore proposes that increased privacy protections should be enacted as part of the Open Banking regime, a proposal which is supported later in this submission.

29. However, the increased risks created by Open Data also require increased regulatory powers and penalties if these protections are to be more than assurances on paper. **It is not realistic to expect consumers to detect data breaches or misuses of their personal information, or to pursue action against those who have exposed or misused their personal information.** Consumers lack the resources, skills and powers necessary to discover most abuses or take effective action in response. Further, to the extent that advanced analytic technologies or artificial intelligence tools are involved in some aspect of the risk manifesting, the technical knowledge

[15] Final Report, 50.

needed will grow over time as these become ever more sophisticated and embedded, and data set proliferation creates ever greater opportunity for them.

30. If the necessary privacy and consumer protections are to have teeth, the relevant regulator will need broad powers to:
    - monitor and audit compliance, over a long time scale consistent with long term persistence of data and the potentially long delays before risks are manifest and, and, geographically, on a global scale, consistent with the global cloud based distribution of data;
    - investigate potential breaches, including breaches of protection and de-identification methods as well as the data itself; and
    - bring representative actions on behalf of affected customers, or support actions if they are conducted under the privacy tort which is the essential precondition for trust in this new regime.

31. The legislation should also include penalties which are sufficient to create the necessary deterrent effect, having regard to the potential for harm and the relatively small chance of most data breaches and misuses being discovered, as explained below. Legislation addressing Open Data should explicitly address the problem of holding accountable those in the chain of custody who should bear responsibility, including those who may have wrongly or recklessly disclosed the data in the first instance. By its nature, the Open Data model tends to diffuse responsibility and invites a lack of concern by those responsible for disclosure and distribution. The remedies need to reduce these effects and undermine expectations of impunity once the data has left one's hands.

Aggregated Data and Retention of Customer Data – Recommendation 3.5

32. In relation to recommendation 3.5, the Final Report states that:

    > Fortunately, if transaction data is within the scope of Open Banking, it will not be necessary to include aggregated data in order to allow others to unlock its value.

As competitors acquire transaction data at the direction of customers, they should be able to replicate the aggregations (at least to some degree) over time.

33. Later, in relation to recommendation 4.3, the Final Report states that:

> Once the customer consent is withdrawn or expires, a customer would reasonably expect that their banking data would be deleted or destroyed in order to protect their privacy.

34. This submission supports the latter view that a customer's personal information should be deleted or destroyed once their consent expires or is withdrawn. The earlier statement, in respect of recommendation 3.5, should be clarified. There should be no expectation that customer data will be retained and aggregated over time.

35. If the intention is that the relevant data would be de-identified, there is a need for consultation on the feasibility of such de-identification and whether it adequately protects a customer who has shared their personal information for a limited purpose. The presumption should be that methods of de-identification will be reduced in effectiveness over time, and most will ultimately fail, so any reliance on them should come with very clear and unavoidable liability for this foreseeable and predictable mode of data breach. It is likely that over time de-identification will be deprecated as a method for data protection, and more restricted and reversible holding methods, and minimisation, will become the norm for safe handling.

Data Recipients Should All be Subject to Privacy Act – Recommendation 4.1

36. This submission supports the recommendation that all data recipients under Open Banking must be subject to the *Privacy Act* (Recommendation 4.1), although this measure alone would not provide adequate privacy protection. This extended application of the *Privacy Act* would impose the same obligations on all data recipients to protect customer privacy, even where the data recipient is classified as

a small business and therefore currently exempt from the application of the *Privacy Act* (with limited exceptions). This is appropriate having regard to both the need to protect customers in the Open Data context and the need to create a level playing field between providers, having increased ease of entry and expansion in the market.

37. The application of the privacy law to small businesses is consistent with the approach of other jurisdictions, including, for example, Canada and the European Union.[16] In fact, the general exemption of small businesses under the *Privacy Act* is likely one reason Australia would not currently qualify for an adequacy assessment under the EU regime. As Australian businesses discover that de facto compliance with the type of protections provided by the EU General Data Protection Regulation are the new global standard, the exemption of small businesses will be decreasingly viable as a regulatory position.

Minimum Modifications to Privacy Protections – Recommendation 4.2

38. This submission supports the recommendation that the privacy protections applicable to Open Banking should be modified as suggested in Table 4.1 of the Final Report (Recommendation 4.2) **as the minimum** increase in protection necessary in the context of the increased risks of the Open Data regime.

39. As noted earlier in this submission, the Final Report rightly acknowledges the increased risks created by the greatly increased collection, storage, transfer and disclosure of personal information contemplated under the Open Data regime. The weaknesses of Australia's current privacy legislation are well-documented. **It is unsafe to promote a revolutionary increase in the exposure of the personal information of Australians without proportionate increases in the legal protection of that personal information**. This submission advocates increased substantive privacy protections, broader application of those protections, greater supervisory,

[16] See *Personal Information Protection and Electronic Documents Act* (SC 2000, c 5) s 4.

investigative and representative powers for the relevant regulator, and penalties which are sufficient to achieve appropriate deterrence.

40. It is important to appreciate that these measures are not simply a means of placating consumers to encourage acceptance of the proposed Open Data regime. Chapter 4 of the Final Report is titled, “Safeguards to inspire confidence”. This title recognises that, if consumers mistrust the Open Data regime, and therefore withhold or distort information or refuse to participate at all, the Open Data goal of increasing the amount and accuracy of personal data available to firms will suffer. Perhaps a more apposite title for this chapter would have been, “Increased protection to avoid net detriment to consumers”. More important than the goal of engendering support for the proposed Open Data regime is ensuring that consumers do not suffer a substantive net detriment from the implementation of the Open Data regime. It is this imperative which should inform the enactment of improved privacy and consumer protections (including the ‘privacy tort’) as a precondition for the implementation of Open Banking and Open Data.

Right to Delete – Recommendation 4.3

41. This submission does not support the recommendation that a right to deletion should not be included in the privacy protections enacted as part of the Open Data regime. Rather it supports the view of the Joint Submission by the Financial Rights Legal Centre and Consumer Action Legal Centre that a right to deletion is integral for the Open Data regime to work as currently recommended by the Report and must form part of the Consumer Data Right.

42. Trust of and participation in an Open Data regime would be something that a prudent advisor would caution against if there were no capacity to effectively revoke consent: if the only option to mitigate the acknowledged much greater data risk is effectively to refuse to ever participate from the start. Consumer advocates would also have more grounds for refusing to endorse the implementation of the scheme if it lacks this basic failsafe. The option for revocation and deletion is thus a useful

fundamental system design requirement. **The ability to withdraw consent is also a beneficial discipline on the data holder or user: they have much greater incentive to retain the trust of data subjects if revocation is possible.** Further, it is technically more feasible than once may have been the case, especially if it is introduced as a core and universal requirement, not an add-on hack, exception, or modification later on.

Customer Consent – Recommendation 4.4

43. This submission supports the recommendation that a customer's consent under Open Banking must be explicit, fully informed and able to be permitted or constrained (that is, unbundled) according to the customer's instructions (Recommendation 4.5), **as a minimum** for the reliance on consent as a justification for data practices. This is to acknowledge that the current approach to consent under the *Privacy Act* is wholly inadequate and requires at least these improvements.

44. At present, we participate in a farce.[17] We claim that businesses give individuals notice about how their personal information will be collected, processed, used and revealed to other entities, and that individuals then make a decision about whether they consent to this treatment of their personal information.

45. In fact, there is often no real notice and there is no real choice in these matters. Individuals routinely make the decision not to read the privacy notices presented to them. This is generally, and wrongly, portrayed as a failing on the part of individuals, with implications of laziness, apathy and an undue attachment to convenience. In fact, individuals make an entirely rational and appropriate decision not to read privacy notices, given:

[17] See also Gordon Hull, 'Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data' (2015) 17 *Ethics Inf Technol* 89.

- the impossibility of making the time (six working weeks per year)[18] necessary to read all privacy notices presented to the average individual;
- the impossibility of understanding the terms of the privacy notices, which are deliberately drafted in broad, open-ended and opaque terms, let alone the consequences of those terms for the individual;[19]
- the absence of any opportunity to negotiate for better terms or to separate certain necessary uses of personal information from other exploitative uses of personal information, given the unilateral, take-it-or-leave-it nature of the notices;[20]
- the absence of effective legal remedies like a cause of action for serious intrusion of privacy, which might be enlivened by unacceptable terms; and
- frequently, the absence of choice in using the relevant service at all, for example, for attendance at schools, participation in sports and events.

46. If individuals are not receiving real notice and make no real choice, their personal information is currently being collected and used without their real consent. There is no 'privacy paradox'. **The fact that consumers continue to use social media, apps, retailer rewards programs and online services in spite of exploitative privacy terms does not reveal a preference for exploitative privacy terms** unless it can be shown that consumers are aware of what those privacy terms are and what they mean; are fully able to gauge the consequences of the proposed data practices; and have a meaningful choice about whether they accept those data practices and their consequences. These conditions are cumulative. So long as consumers cannot absorb, understand or make a choice about exploitative privacy terms, their continued loyalty to the firms that produce them reveals nothing but the relative impotence of the consumer.

[18] AM McDonald and LF Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 *A Journal of Law and Policy for the Information Society* 540.

[19] Including the absence of critical concrete details, such as the names of all of the companies which may access the data, or a means to find them.

[20] The typical absence of a right of revocation means that checking a privacy policy again later when the reader is more familiar with the realities and implications offers no benefit.

47. At present, it is lawful for firms in Australia to require consumers to accept broad, open-ended uses and 'sharing' or disclosures of their personal information well beyond the purpose for which that personal information was originally provided, as a condition of receiving a certain service, undermining the original aim of what is now Australian Privacy Principle 6 to limit use and disclosure by reference to purpose of collection. It is lawful for this "consent" to be implicit, in the sense that the consumer's continued use of a service or website can be taken as acceptance of these terms in the absence of any express agreement.

48. If Open Banking is implemented without improvements to current protections under the *Privacy Act*, the most likely outcome is that when a customer requests the transfer of their personal information from their bank to a third party data recipient, that third party data recipient will require the customer to accept a standard form agreement (to tick a box indicating "I agree with the terms and conditions") which will include the customer's consent to broad, open-ended uses and sharing of their personal information well beyond the purpose for which that personal information is provided, as a condition of the customer making the credit application or receiving the budgeting app or the mortgage comparison service. In this way, Open Banking would facilitate vastly increased exposure of customers' personal information without any real consent and against their interests.

49. **It is critical that any customer consent to data practices under Open Banking is voluntary, unbundled, explicit, fully informed, time limited, revocable and requires action on the part of the customer**. Further, data recipients should only collect the minimum personal information necessary to provide the service requested by the consumer. At the same time, it should be understood that, internationally, scholars, regulators and policymakers are increasingly questioning the acceptance of consent as a primary justification for data practices, particularly given the increasingly complex uses of personal data, and consequences of those uses, in the age of big

data and algorithmic decision-making. In short, the proposed uses and their consequences may be well beyond the comprehension of consumers.[21]

Allocation of Liability and Penalties – Recommendation 4.9

50. This submission generally supports the allocation of liability proposed in Recommendation 4.9 of the Final Report, but argues the proposed allocation of liability and existing penalties under the *Privacy Act* are inadequate to compel firms to take appropriate protective measures in the context of the Open Data regime.

51. There should be provision for severe penalties in the event of data breaches, breach of de-identification method, and unauthorised access and use of personal information, including those which arise as a result of 'sharing' data with third parties with inadequate protections in other jurisdictions. In setting such penalties, it is necessary to take into account:
    - the increase in such risks created by the proliferation of data collection, use, processing and transfer inherent in the Open Data regime;
    - the relatively small chance that the relevant breaches and misuses will be discovered by consumers or regulators; and
    - the expense and difficulty of bringing enforcement or litigious action in response.

52. Further, these **penalties should create potential liability which is sufficiently severe that firms do not simply price the contingency into their business model but instead take the utmost measures to protect consumer data, in line with consumer interests**.[22] In addition, there must be moves to reduce the expense and difficulty of enforcement or litigation, by means for instance of passage of the privacy tort, so

[21] See, eg, Office of the Privacy Commissioner of Canada, 'Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent under the *Personal Information Protection and Electronic Documents Act*' (Report, 2016).

[22] The critical case is where risk of breach is high: it should not make governance or risk management sense to a firm to proceed with a project or disclosure where they cannot assure protection, on the basis that risk to them of enforcement or litigation is in practice minimal, as it is at present. It should also not make sense for data to be released because the releasing party assumes that any breach will occur so far into the future that they will not be held accountable.

there is a litigation risk at all; presumptions against the releaser in certain circumstances, or reduced evidentiary burden on the victim or regulator; and facilitation of class actions, including funding support and indemnity mechanisms, particularly given the large number of people likely to be affected by the same harm under an Open Data regime and the low incentive for any individual to sue alone.

Transparency – Recommendation 5.11

53. This submission supports the recommendation that customers should be able to access a record of their usage history and data holders should keep records of the performance of their API that can be supplied to the regulator as needed (Recommendation 5.11). This access and record-keeping would be a basic requirement for appropriate monitoring of data transfers.

54. It should also extend to long term retention of these detailed logs. It should extend to a lifetime tracking of the data set as it passes through other hands, to show provenance, locate the first discloser and all subsequent disclosers, facilitate audit and discovery, and oversight of data set lifecycle. At present there appear to be expectations that Open Data will be 'release and forget', with the originator wanting to be no longer be associated with the data once it is out of their hands. Open Data should come with a metadata and logging requirement, whereby critical information stays attached to the data set for life. Removing such attribution and provenance metadata must be both an offence and breach of the terms of use, triggering immediate revocation of licence.

55. It is critical to have a bright line between responsible and controlled Open Data use, and clear abusive practices, so there is no doubt when someone crosses the line. This sort of metadata and provenance tracking requirement will help avoid 'laundering', losing data, and trafficking improperly in such data sets, and will provide incentives for all involved in handling such data to recognise that they will remain accountable.

Timing and Implementation: Chapter 6

45. The proposed rule-making should take place in **consultation** with relevant stakeholders prior to the more technical standard-setting by the Data Standards Body, which is to add detail to the norms and principles established by the rules. With regard to **timing**, while these two processes may overlap in time, the rule-making should take the lead if the proposed hierarchy of regulation is intended to be meaningful.

46. As noted earlier, the passage of the long overdue privacy tort must be a condition prior to any legislative action implementing an Open Banking, or Open Data, regime. This privacy tort can be introduced as a statutory cause of action for serious intrusion of privacy, as recommended by ALRC in 2014 after a decade of consultation. Failing to legislate for this tort would expose consumers to increased risk while not addressing the great defect in Australia's data protection regime, and would fundamentally undermine any hope of demonstrating a trustworthy environment for Open Data, or achieving substantial support for the model.