THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Treasury Laws Amendment (Consumer Data Right) Bill 2018 – Exposure Draft

September 2018

Daniel McAuliffe
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600

By email: data@treasury.gov.au

Contact: **David Turner**
President, NSW Young Lawyers

Irene Halforty
Vice-Chair, NSW Young Lawyers Communications, Entertainment and Technology Committee

Contributors: Ashleigh Fehrenbach, Irene Halforty, Onur Saygin, Sophia Urlich and Eva Yi Lu

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

NSW Young Lawyers Communications, Entertainment and Technology Law Committee makes the following submission in response to the Treasury Laws Amendment (Consumer Data Right) Bill 2018.

NSW Young Lawyers is a division of The Law Society of New South Wales. NSW Young Lawyers supports practitioners in their professional and career development in numerous ways, including by encouraging active participation in its 15 separate committees, each dedicated to particular areas of practice. Membership is automatic for all NSW lawyers (solicitors and barristers) under 36 years and/or in their first five years of practice, as well as law students. NSW Young Lawyers currently has over 15,000 members.

The Communications, Entertainment and Technology Law Committee (**Committee**) of NSW Young Lawyers aims to serve the interests of lawyers, law students and other members of the community concerned with areas of law relating to information and communication technology (including technology affecting legal practice), intellectual property, advertising and consumer protection, confidential information and privacy, entertainment, and the media. As innovation inevitably challenges custom, the CET Committee promotes forward thinking, particularly about the shape of the law and the legal profession.

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Overview

The Communications, Entertainment and Technology Law Committee (**Committee**) of NSW Young Lawyers welcomes the opportunity to comment on the Exposure Draft of the *Treasury Laws Amendment (Consumer Data Right) Bill 2018* (**CDR Bill**).

The CDR Explanatory Material states that the CDR "will provide individuals and businesses with a right to efficiently and conveniently access specified data in relation to them" and that it is "designed to give customers more control over their information." The Committee is broadly supportive of initiatives to increase greater participation and control by consumers of their data in a manner that produces greater competition and consumer/individual outcomes.

However, greater 'open data' or data sharing raises legitimate concerns about privacy, data ownership and responsible and ethical data practices. The Committee submits that the proposed benefits to individuals/consumers can only be achieved with a strong and consistent emphasis on data safeguards, privacy protections and public trust to avoid repeating recent examples of data practices that are inconsistent with consumer expectations and which have eroded consumer/individual privacy and their trust in greater open data and data use, such as, for example, the data practices of Cambridge Analytica/Facebook and Health Engine.

In addition, the Committee refers the Treasury to its recent submission made to the *Department of the Prime Minister and Cabinet* in response to the proposed Data Sharing and Release Legislation Issues Paper (**DS&R Submission**). The Committee's DS&R Submission stressed that "the development and consideration of any Data Sharing and Release Bill should not occur in isolation to other data access regime, such as the development of the 'Consumer Data Right' currently being overseen by the Treasury." The Committee is of the view the resulting implications to individuals' privacy are exponentially greater when these two regimes are combined than when they are considered in isolation. As such, the Committee submits that the Treasury have regard to other data access and sharing regimes currently being developed or implemented by the Government when considering the privacy implications to individuals/consumers.

1. Designated Sectors, Participants, and the Accreditation Process

The Committee notes that the CDR is intended to first be implemented in the banking, energy and telecommunications sectors, and is expected to be introduced economy-wide in the future. The Minister will designate the sectors to which the CDR will apply. Proposed subsection 56AD(1) outlines several considerations that the Minister needs to make before designating a sector to the CDR.

The Committee welcomes the emphasis that has been placed on privacy considerations, as well as the promotion of competition and data-driven innovation. The Committee raises the following concerns:

a) privacy considerations may be limited to the CDR context as opposed to consideration of privacy more broadly (ie. 'privacy considerations' may not account for the cumulative impact of the various data sharing and access regimes currently being developed and implemented by the Government);

b) the appropriateness and utility of applying a single Consumer Data Right Framework (**CDRF**) across the economy with a diverse range of sectors, businesses, and activities and data sets (ie. different sectors of the economy are subject to different regulations and collect, hold and use different types of data – some of which may not be possible, desirable or useful to be subject to the CDR. For example, health data);

c) Consumers in the CDR system will include individuals as well as small, medium or large businesses. The Committee notes the current small business exception under the *Privacy Act 1988* (Cth) (**Privacy Act**) and recommends that the appropriateness of this exception be reconsidered, notwithstanding the requirement under the CDR Bill for small businesses that become accredited data recipients to comply with privacy laws. The Committee considers that the CDR Bill would not address privacy issues and compliance relating to the personal information collected by small businesses that later become accredited data recipients. i.e. small businesses can currently collect a lot of personal information without any need to comply with the Privacy Act and this data may be subject to the CDR in the future if the small business becomes accredited;

d) The Committee submits that a strong and consistent emphasis on data safeguards is required and recommends that both data holders and data recipients be subject to the accreditation process. In addition, the Committee submits that it is appropriate to require all data holders and data recipients that participate in the CDR be subject to rigorous data safeguards and privacy protections.

e) The Committee notes the scope for consumers to transfer certain data out of the CDR system and for non-accredited entities to participate in the system and gain access to certain data in certain circumstances.[1] The Committee is concerned about the paucity of detail provided in relation to these issues and recommends that further detail be provided in this regard, as well as consultation.

f) Proposed section 56CE(1) provides that the Data Recipient Accreditor (initially the Australian Competition and Consumer Commission (**ACCC**)) may accredit a person if the person satisfies criteria specified in consumer data rules relating to the accreditation of data recipients. The Committee is particularly concerned about the lack of detail provided in relation of the criteria that persons will need to satisfy to become accredited as data recipients, as well as the broad scope of persons who are eligible to seek accreditation.[2] At this stage, it is not clear what criteria a person will need to satisfy in order to become accredited, particularly because the criteria, and the technical standards to support them, are yet to be formulated. The Committee submits further detail is required and submits that all data holder and data recipients participating in the CDR must adhere to minimum data safeguards and privacy protections.

2. Consumer Data Rules

The CDR Bill empowers the ACCC to make rules (**Consumer Data Rules**) for designated sectors. The proposed section 56BB of the *Competition and Consumer Act (2010)* (**CCA**) sets out the matters which the Consumer Data Rules may deal with. These are:

a) disclosure, use, accuracy, storage, security or deletion of CDR data for which there are CDR consumers (with additional details in section 56BC);
b) disclosure, use, accuracy, storage, security or deletion of CDR data for which there are no CDR consumers (with additional details in section 56BD);
c) accreditation of data recipients (with additional details in section 56BF);
d) reporting and record keeping (with additional details in section 56BG);
e) matters incidental or related to any of the above matters (with additional details in section 56BH).

While these proposed sections provide some framework to what the Consumer Data Rules will address for each designated sector, much of the detail is to be developed by the ACCC.

[1] Section 1.47 Explanatory Materials to the Draft Exposure Bill.

[2] Section 56CE(2) of the Draft Exposure Bill provides that a person need not be a registered company nor an Australian citizen or permanent resident to become accredited.

The Committee submits that rules will need to be adapted to particular sectors; given that any sector may become a designated sector in the future and the different types and utility of data held by each sector, it will be difficult to prescribe a single set of rules. However, insufficient detail creates uncertainty and provides little insight into how the Consumer Data Rules will operate in practice. The Committee is of the view that it is possible to provide some minimum requirements that cannot be derogated by the Consumer Data Rules. For instance, the CDR Bill should include minimum storage and security requirements, minimum reporting and record keeping requirements, and a basic framework for the accreditation process.

It is also unclear whether the Consumer Data Rules for each sector will have the ability to narrow the broad definition of CDR data in the proposed section 56AF. CDR data is proposed to be defined as information that is specified in an instrument designating a sector, as well as any information derived from that designated sector data and any information derived from that derived information, and so on. This cascading effect would likely capture a broad range of value-added data sets. This may have the unintended consequence of discouraging industry and businesses to invest in data and innovative data analysis and use, as the value-added data (ie. the output of their investment) may be subject to the CDR to the benefit of competitors. In the long term this may reduce new innovative products and services that benefit consumers.

The Committee seeks further clarification on the scope of the CDR, including whether value-added data will be subject to the CDR. The Committee recommends that as first preference, the definition of CDR be narrowed to exclude information derived from derived information or alternatively, the ACCC be granted the power to limit the data that can be subject to the Consumer Data Right and the Consumer Data Rules.

The Committee also notes the difficulty of managing the multi-tiered compliance under the Privacy Act and the new privacy safeguards (discussed below) given the broad definition of the CDR data. The Committee supports the proposed section 56EC of the CCA, which provides if there is an inconsistency between the privacy safeguards and the Consumer Data Rules, the safeguards prevail over the rules to the extent of the inconsistency.

The lack of details in the current CDR Bill about the Consumer Data Rules means it is crucial that a robust public consultation process is conducted for every designated sector. The proposed section 56BO(1) of the CCA provides that before the Consumer Data Rules are made for a sector, consultation with the following parties are required:

a) the public;
b) the Information Commissioner;

c) if the proposed rules relate to a particular designated sector – the person or body (if any) that the Commission believes to be the primary regulator of that sector; and
d) any person or body prescribed by the regulations for the purposes of this paragraph.

The Committee suggests that if there is no primary regulator as described in (c), the Commission should conduct in-depth consultation with the entities that fall into the sector.

The proposed section 56BO(2) provides that when consulting with the public, it would be sufficient to make available the proposed Consumer Data Rules or a description of the content of the proposed Consumer Data Rules on the website and invite the public to comment on the proposed rules (emphasis added). The Committee submits that the provision of a description only may result in ambiguity in interpretation, and instead prefers that the full text be made available for consultation so consumers can understand the full scope and context.

The Committee notes that under proposed section 56BQ(1), the Commission can make Consumer Data Rules in an emergency, after consulting the Information Commissioner (but no other parties); and without the consent of the Minister, if the Commission is of the opinion that it is necessary, or in the public interest, to do so in order:

(a) to protect the efficiency, integrity and stability of any aspect of the Australian economy; or
(b) to avoid imminent risk of serious harm to consumers.

The Committee also notes that under the proposed section 56BQ(4), where “emergency” rules are made under this provision, unless the Minister makes a direction about those rules, they will cease to be in force 6 months after the date the rules were made.

The Committee is concerned that the CDR Bill provides extensive carve outs (such as the one noted above at s56BQ(1)) which result in many of the consultation processes being bypassed. In particular, the Committee is apprehensive about the wide range of instances that could constitute the protection of the "efficiency, integrity and stability of any aspect of the Australian economy." There is also no detail as to what would constitute "imminent risk of serious harm to consumers." The Explanatory Material also does not provide adequate guidance on what this term means.

The Committee recommends that unless definitive examples can be provided that would require such urgent action to explain these exceptions, the CDR Bill should not, in any circumstances, provide an exception to

consultation with the Information Commissioner.[3] The Committee also suggests that instead of providing an exception to consultation, the Commission could instead be provided with a power to review or put a stay on a data disclosure in such emergency situations.

In relation to remedies, the ACCC will have the power to designate a civil penalty provision (proposed section 56BJ of the CCA) if there has been a breach of part or all of the Consumer Data Rules. However, the nature of those offences have not been specified.

The proposed section 56GC(2) of the CCA seeks to provide some comfort for data holders. This is evidenced by stating that if a "CDR participant" provides CDR data to another person in accordance with the relevant requirements, including the Consumer Data Rules, the "CDR participant" will not be liable to a civil or criminal action, for or in relation to that conduct. The Committee is uncertain how this will operate in practice where the data holder is in breach of other provisions of the CDR. The Committee is however supportive that the CDR Bill makes it a criminal offence and a civil penalty provision to engage in certain misleading or deceptive conduct in relation to the Consumer Data Right.[4]

3. Privacy Framework

The Committee broadly supports the specific focus on protecting the privacy of consumers. It also supports the expansion of privacy protections under the CDR beyond the Privacy Act to data that 'relates' to an individual. The Committee notes that the Consumer Data Rules are likely to provide more sector specific privacy protections. Notwithstanding these, the Committee submits that fundamental privacy protections should be codified within the CDR Bill.

The Committee submits that an unambiguous identification of the rights consumers have with respect to the use of their own CDR data is essential.[5] Ambiguity is likely to reduce the value and bargaining power that a consumer could otherwise derive from the introduction of a CDR.

The Committee questions whether the appropriateness that complete records of industry sector specific data sets should be transferred upon request generally from one accredited data recipient to another. Privacy Safeguard 10 requires CDR participants to transmit all, and not part, of the information a consumer wishes to

[3] Section 56BQ(3) of the Draft Exposure Bill

[4] Section 56BM of the Draft Exposure Bill

[5] For example, a consumer that wishes to protect their privacy may wish to only permit transfer of a portion of a data set or opt to reduce the level of detail in a dataset before transmitting it.

transmit. The Committee submits that consumers and individuals should have the right or ability to specify that only parts the CDR data is to be transmitted. The proposed wording of Privacy Safeguard 10, particularly the phrase 'complete' may stifle the opportunity for the privacy preserving trade-off that is possible between allowing CDR participants to access or monetise CDR data, and allowing consumers to have the choice and control to disclose the minimum amount of information required for there to be a mutual benefit. Privacy Safeguard 10 as proposed may have the consequence of inhibiting flexibility for consumers to choose the level of detail they wish to share.

The Committee further submits that the CDR Bill should contain an express prohibition on refusing services or products to a consumer or individual on the basis of refusing to agree to a CDR data transfer. This is in addition to requesting a transfer of CDR data where this data is not reasonably necessary to provide a consumer with competing services or products. For example, an accredited data recipient may request CDR data from an individual as a pre-condition to offering a competing service, notwithstanding that the CDR data may not be necessary for, or relate to, the purpose for which a consumer or individual engages or transacts with the accredited data recipient.

The Committee also submits that stronger protections are required to address the significant privacy implications both for the consumer consenting to a transfer of CDR data and for third parties who do not explicitly consent to that transfer. The Committee is concerned that this issue has not been specifically addressed under the CDR Bill. The impact of inadvertent or residual disclosures about third parties should be carefully considered from a privacy perspective. The Committee recommends that further information be provided in relation to the collection and use of personal information of third parties as the result of CDR data-practices (ie. combination and analysis of various CDR data sets).[6]

In order to allow a consumer to make an informed decision as to whether to consent to the transfer of CDR data, and the impact upon their privacy should that transfer occur, the Committee further recommends that accredited data recipients be required to:

- disclose to the consumer the CDR data relating to that consumer that it is already in its possession. This is in addition to any other data relating to the consumer that it intends to combine with the CDR data; and

[6] It is noted that EDB, s56EH (PS 5) refers to 'collects CDR data' but does not identify how and when the act of combining two or more CDR data sets will be considered 'a collection' of information giving rise to the obligation to notify the CDR consumer.

- provide an inference warning about the type of additional insight the accredited data recipient is likely to be able to deduce.

The Committee supports the current and time limited consent requirement as indicated in Consumer Data Right Privacy Protections document.[7] However the Committee is of the view that such a critical aspect of the CDR should be contained within the primary statute rather than left to the Consumer Data Rules. The Committee views the Consumer Data Rules as the appropriate vehicle to shape the extent of when consent lapses or needs to be renewed by the consumer. Despite this, given the differences between industry sectors, omitting the necessity for current and time limited consent as a stipulated inclusion of the Consumer Data Rules in the CDR Bill significantly diminishes a vital protection of consumer privacy. This is because it does not require the Consumer Data Rules to include such protections.

The Committee supports the intended purpose of Privacy Safeguard 11[8] subject to concerns the current drafting of the provision is inadequate as it does not specify lapsing or revocation of consent as alternative events requiring a person in possession of CDR data to delete that data.[9] The Committee is of the view that the control mechanism of deletion is vital to enable consumers to protect their privacy from the risk of misuse and data breaches.

In addition, the Committee is concerned about the relegation of guidance on how to interpret 'de-identified' to the Exposure Draft Explanatory Materials.[10] This definition has significant implications for consumer privacy given that a person who has CDR data they no longer need, can opt to 'de-identify' it rather than delete it. In its current form, it is unlikely any CDR data would be deleted if in the 'de-identified' form it carried any value.[11]

Unless de-identification is defined clearly in the legislation, a reference to it is highly problematic. The conventional approach of removing identifiers such as name, address, date of birth from collected data which contains or concerns intimate details of people's lives (such as when and where they conducted credit transactions or when, where and whom they called or texted) is a form of de-identification that is inadequate.

---

[7] Particularly the discussion at page 2 which accompanies the title 'Genuine Consent' https://static.treasury.gov.au/uploads/sites/1/2018/08/Consumer_Data_Right_Privacy_T316972.pdf

[8] Section 56EN of the Draft Exposure Bill.

[9] "Rights to withdraw or delete" was specified as an important part of the CDR in the document titled Consumer Data Right Privacy Protections https://static.treasury.gov.au/uploads/sites/1/2018/08/Consumer_Data_Right_Privacy_T316972.pdf.

[10] See https://static.treasury.gov.au/uploads/sites/1/2018/08/Consumer_Data_Right_EM_T316972.pdf at 1.173.

[11] The Committee also notes that the less de-identified CDR data is, the more likely it is to carry value, encouraging persons seized with CDR data to override the protection intended by this provision at a cost to consumer privacy.

The conventional process of cross referencing can reveal the identity of the consumer to whom the data belongs. These kinds of processes are likely to be made more readily accessible in the future.

Furthermore, stakeholder certainty in relation to how to comply with the CDR Bill is likely to be reduced if further guidance is not provided. The Committee recommends that the definition of de-identification[12] should be extended to ensure that all copies of the redundant data are permanently transformed into a state from which they can no longer be used to identify the consumer to whom it relates. This should take into account (a) the capacity for anonymity inherent to the type and scope of data and (b) accounting for public and commercially available datasets and analysis tools which could be utilised to reconstitute the redundant data.

The Committee supports and recommends the inclusion of private remedies for consumers/individuals, as was noted as a CDR privacy protection in an earlier document released by Treasury.[13] The Committee considers it important to provide aggrieved consumers and individuals who have suffered a breach of their privacy by non-compliance with the CDR with an ability to seek relief independently of enforcement agencies and in addition to ability to make complaints to the relevant enforcement agency. The Committee considers that in the context of the growing importance of consumer data and future CDR participants increasingly relying on data relating to individuals when making decisions which affect them, providing consumers with private remedies is incredibly important. This is because of the significant impact incorrect or unauthorised data can have upon an individual's life. This risk of litigation would also further incentivise CDR participants to comply with their obligations under the Consumer Data Right Safeguards Framework.

The Committee is of the view that irrespective of prior standing consent given by a consumer, organisations which have CDR data in their possession from any source (other than directly from a consumer) should be required to inform the consumer the CDR data sets that were relied upon, upon request by that consumer. This information should be able to be interpreted by all consumers and easily allow the consumer to access it. Without such a requirement, there is a high risk that consumers that are denied certain products because of their CDR data (especially where that data is erroneous or is available due to a mistake) will be additionally disadvantaged. This would be due to the additional time and resources they need to expend to identify the specific CDR data which was relied upon by the CDR participant making the decision. One way in which this could be achieved would be by extending Privacy Safeguard 5[14] to have the effect that a CDR participant that

[12] Section 56EN(2) [final paragraph] of the Draft Exposure Bill.

[13] "Direct rights of action" was specified as an important part of the CDR in the document titled Consumer Data Right Privacy Protections https://static.treasury.gov.au/uploads/sites/1/2018/08/Consumer_Data_Right_Privacy_T316972.pdf.

[14] Section 56EH of the Draft Exposure Bill

is in possession of CDR data should not be able to use that data until reasonable steps to notify consumer of that use have been undertaken.

The structures and processes in relation to this new proposed system should be clearly outlined so that consumer confusion is minimised. Consideration should be given to ensuring minimal duplication and ensuring clear delineation of roles and responsibilities for regulatory bodies. Consumers should also be educated to understand where to go to make a complaint.

Finally, the Committee recognises that the CDR and educational campaign designed to increase consumer awareness of the CDR will play a critical role in achieving the privacy outcomes targeted for the Consumer Data Right Safeguards Framework. However, care should be taken in relying too heavily on these future steps during the drafting of the CDR Bill. Particular care should be employed to minimise the complexity that arises from interactions between the CDR Bill, the Privacy Act and CCA.

Concluding Comments

NSW Young Lawyers and the Committee thank you for the opportunity to make this submission. The Committee would welcome further consultation opportunities on a more detailed level.

Please note that the views and opinions expressed in this letter are on behalf of the Committee and its authors/contributors and do not reflect the views or opinions of any employer or company related to the authors and/or contributors.

If you have any queries or require further submissions please contact the undersigned at your convenience.

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Contact:

David Turner

President

NSW Young Lawyers

Email: president@younglawyers.com.au

Alternate Contact

Irene Halforty

Vice Chair

NSW Young Lawyers Communications, Entertainment and Technology Committee

Email: cet.chair@younglawyers.com.au