THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Submission on the Treasury's Issues Paper – *Inquiry into the Future Directions of the Consumer Data Right*

21 May 2020

Secretariat
Inquiry into Future Directions for the Consumer Data Right
The Treasury
Langton Crescent
PARKES ACT 2600

Email: data@treasury.gov.au

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

Olga Kubyk
Chair, NSW Young Lawyers Business Law Committee

Ashleigh Fehrenbach

Chair, NSW Young Lawyers Communications, Entertainment and Technology Committee

Contributors: Olivia Irvine, Adam Herman, Ara Daquinag, Olga Kubyk, Nick Rose (researcher), Katherine Stapels, Michael Tangonan, Ben Wilson, Emma Ting, Daniel Iminjan, Ravi Nayyar, Melissa Camp, Samantha Ferdous, Chujing Cai, Bob Liang and Mitheran Selvendran.

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

The NSW Young Lawyers Business Law and Communications, Entertainment and Technology Committees make the following submission in response to the Treasury's Issues Paper (March 2020) – *Inquiry into the Future Directions of the Consumer Data Right.*

NSW Young Lawyers

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 16 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.

NSW Young Lawyers Business Law Committee

The Committee comprises a group of approximately 1,700 members in all aspects of business law who have joined together to disseminate developments in business law and foster an increased understanding of business law in the profession. The Committee reviews and comments on legal developments across corporate and commercial law, banking and finance, superannuation, taxation, insolvency, competition and trade practices, among others.

NSW Young Lawyers Communications, Entertainment and Technology Law Committee

The Committee 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 Committee promotes forward thinking, particularly about the shape of the law and the legal profession.

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Introduction

The Committees welcome the opportunity to make a submission concerning the inquiry and the ways in which the Consumer Data Right ("**CDR**") could be leveraged to enhance competition and advance the development of a safe and efficient digital economy for the benefit of Australians.

In short, the Committees recommend that:

1. the CDR Rules should prescribe:
   (a) limits to the types of products and services that may be recommended using data derived from the CDR; and
   (b) additional privacy safeguards to ensure user confidence in the CDR is not undermined a lack of recourse as a result of a data privacy breach.
2. consumers should be informed of data security implications of transferring data to non-accredited firms;
3. accredited data recipients be required to disclose the CDR data relating to the consumer that is already in its possession, in addition to any other data relating to the consumer that it intends to combine with the CDR data;
4. the definition of de-identification should be extended to require that all copies of the redundant data be permanently transformed into a state from which they can no longer be used to identify the consumer to whom it relates;
5. data holders and recipients should, if a data breach is identified, be under an obligation to halt at-risk services until the breach is rectified, notify an appropriate regulatory body (with penalties for non-compliance to discourage concealment), and be liable for any damages caused to consumers;
6. private remedies should also be available for individuals in respect of data misuse (for example privately-recoverable pecuniary penalties), in addition to enforcement by the relevant enforcement agency.

Below, the Committees outline the ways in which those themes are relevant in relation to the terms of reference.

Future Role and Outcomes of the Consumer Data Right

Consumer convenience

The Committees submit that the enhanced ability of consumers to switch between service providers makes consumer retention ever more important, which incentivises businesses to adopt transparent systems and processes and build business models that focus on creating additional value for consumers.[1] On the flip side, the increasing autonomy over data may create unintended complexities. Data-holders may learn news ways of deriving value from the existing consumer data,[2] and, if those are monetised, the consumer entitlements to a share of profits derived from the use of data about them by data holders would require considerable thought.

Extension to other industries

The Committees note that the CDR's role in connection with consumer data is distinct from that in connection with product information.

The Committees submit that in order to develop a fully functioning CDR framework, which does not produce unintended economic consequences and proves most beneficial, the future role of CDR in connection with product information should be limited either to industries that:

a. are regulated with industry-specific regulation;
b. are homogenous; and
c. have access to personally identifiable information of consumers that is linked to certain transactions and spending habits.

The Committees submit that it may not be practical to extend the operation of the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) (the Rules) ("**CDR Rules**") to all sectors of the economy in the sense of making information on various product offerings available, because:

a. not all sectors in the economy supply goods and/or services that are readily substitutable for one another; and
b. market competition is imperfect by nature.

[1] Phuong Nguyen and Lauren Solon, 'Consumer data and the digital economy' (Report, 17 July 2018) <https://cprc.org.au/wp-content/uploads/Full_Data_Report_A4_FIN.pdf>.
[2] Melbourne Law School, 'Australia's Consumer Data Right: Opportunities and Challenges' (YouTube, 22 October 2019) < https://www.youtube.com/watch?v=hizQClbMrQo&t=3330s>.

The Committees submit that the CDR would not have the effect of moving every market closer to 'perfect competition' because maintaining the CDR framework carries a heavy administrative burden associated with implementing and monitoring adherence to any legislation, which is not necessarily supported by the marginal benefit it may achieve.

International Context

The Committees submit that cross-border cooperation with foreign governments, international organisations and fora like the OECD in designing the CDR would help achieve interoperability of national data portability frameworks and would enable Australian consumers to realise the economic potential of their data in both overseas and domestic markets. That is, the Committees support Australia designing its frameworks to be consistent with those used in other markets to the extent possible and otherwise consistent with Australia's policy objectives.

In particular, the Committees support the Treasury's consideration of the CDR developments in the European Union through the adoption of the European General Data Protection Regulation ("**GDPR**").

The Treasury should consider including features that are similar to the following features of the GDPR:

a. The withdrawal of consent is as accessible as the granting of consent.[3]
b. Consumers are required to be informed of the purpose of the collection of data, its legal basis, and the manner in which it would be used.[4] The CDR is an opportunity for the Treasury to expand the rights that already exist under the *Privacy Act 1988* (Cth).
c. Information regarding the consent given by a consumer to a data request is to be provided in a concise, transparent, intelligible, and easily accessible form with clear and plain language. Particular consideration needs to be given to children.[5]

[3] *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* [2016] OJ L 119/1, art 7(3).
[4] *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* [2016] OJ L 119/1, art 13.
[5] *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* [2016] OJ L 119/1, art 12.

Under the GDPR, the data subjects have the following rights that CDR privacy protection should be modelled on:

a. the right to access personal data;[6]
b. the right to erase (right to be forgotten);[7]
c. the right to restrict processing;[8]
d. the right to data portability;[9]
e. the right to reject automated decisions;[10]
f. the right to rectify;[11]
g. the right to restrict data processing; and
h. the right to object.[12]

The Committees submit that, as a part of the CDR framework, consumers should have the right to request the deletion of their data (similar to that which exists under the GDPR) given the CDR's strong focus on data portability. Consumers who choose to transfer their data from one service provider to another risk having copies of their data stored by multiple service-providers, thereby increasing the risks of data breaches.

The Committees submit that it is desirable to implement a standardised format for Application Programming Interfaces ("**API**") and a support framework surrounding the API implementation (or a publicly accessible knowledge database). Open Banking imposes an obligation to use a standard format in software frameworks to ensure compliance. This achieves greater harmonisation of accessibility for consumers across different types of read and/or write permissions and provides organisations with an opportunity to collaborate across industries. Presently, Open Banking provides publicly accessible online resources for the public and developers, including software tools to verify compliance and API specifications.[13] The Committees believe that providing resources, like consumer-friendly information about the specifications (the type of information and how it is transferred), would assist in strengthening public confidence in the CDR, increasing community awareness, and ensuring its widespread use.[14]

---

[6] *General Data Protection Regulation (EU)* 2016/ 679 art 15.
[7] *General Data Protection Regulation (EU)* 2016/ 679 art 17.
[8] *General Data Protection Regulation (EU)* 2016/ 679 art 18.
[9] *General Data Protection Regulation (EU)* 2016/ 679 art 20.
[10] *General Data Protection Regulation (EU)* 2016/ 679 art 22.
[11] *General Data Protection Regulation (EU)* 2016/ 679 art 16.
[12] *General Data Protection Regulation (EU)* 2016/ 679 art 21.
[13] Open Banking, *Frequently Asked Questions*, <https://openbankinguk.github.io/knowledge-base-pub/>.
[14] Productivity Commission, *Data Availability and Use* (Inquiry Report No 82, March 2017) 159-64.

Switching

The Committees submit that the CDR may not be effective in encouraging Australian consumers to switch service providers because of the lack of awareness of alternative services. For example, despite the presence of 'neobanks' in the Australian financial services market, neobanks have not made substantial inroads into the market share of the 'Big 4' Australian banks.[15] The issue is writ large in Nielsen's consideration that: '*Australians aren't quite ready just yet to transition from traditional banking behaviours to a neobank's new mobile-only experience*.' [16] Almost half of the individuals surveyed said 'they had never heard of a neobank'.[17] A CDR allowing Australians to switch their banking providers to neobanks may be of little practical value for so long as many Australians do not know about the range of entities available.

The Committees submit that the Treasury should, in partnership with the Australian Securities and Investments Commission ("**ASIC**"), engage and educate the Australian public about the variety of banking and payment services options available to them (especially about those outside the 'Big 4' Australian banks) and the offerings of the Australian FinTech sector more broadly (as appropriate to the circumstances of communities engaged with). Partnering with the FinTech industry's peak advocacy industry body, FinTech Australia,[18] would assist with removing the behavioural barriers and potentially helping Australians apprehend neobanks' business models, without which consumers are unlikely to switch to neobanks even with the CDR present. This recommendation presupposes the existence of a thriving Australian FinTech sector with businesses that can benefit from the existence of the CDR by using it to potentially gain customers.

The Committees support the continued development of a thriving Australian FinTech sector that produces businesses that can benefit from the CDR by attracting consumers. The Committees welcome initiatives like the enactment in February 2020 of the FinTech regulatory sandbox,[19] which was an outstanding example of the openness of ASIC in working with and providing regulatory guidance to the FinTech sector. Initiatives that support the development of FinTech

---

[15] Clancy Yates, 'Meet the "Neobanks" Trying to Shatter the Big Four Banking Oligopoly', Sydney Morning Herald (online, 17 August 2019) <https://www.smh.com.au/business/banking-and-finance/meet-the-neobanks-trying-to-shatter-the-big-four-banking-oligopoly-20190815-p52hiu.html>.

[16] Jo Brockhurst, 'Will Australians Put Their Money where Their Mouth Is and Switch Banks?', Nielsen (Web Page, 20 November 2019) [1] <https://www.nielsen.com/au/en/insights/article/2019/will-australians-put-their-money-where-their-mouth-is-and-switch-banks/>.

[17] Jo Brockhurst, 'Will Australians Put Their Money where Their Mouth Is and Switch Banks?', Nielsen (Web Page, 20 November 2019) [1] <https://www.nielsen.com/au/en/insights/article/2019/will-australians-put-their-money-where-their-mouth-is-and-switch-banks/>.

[18] FinTech Australia', FinTech Australia (Web Page, 20 December 2019) <https://fintechaustralia.org.au/>.

[19] Jane Hume, Assistant Minister for Superannuation, Financial Services and Financial Technology, 'New Laws Passed to Drive Fintech Innovation and Competition in the Financial Sector' (Media Release, 11 February 2020).

industry, such as the regulatory sandbox, support the creation of an environment for the CDR to flourish.

Read access

The Committees submit that the language for the provision of consent should be standardised and the CDR should provide a standardised and explicit facility for consumers to withdraw their consent, including the ability to request the deletion of previously provided data. Surveys have shown that similar rights available under the GDPR have rarely been exercised.[20] Standardisation would assist consumers with understanding their rights and exercising the same, which, based on the GDPR's experience, is crucial for its effective operation.

Resource limitations

The Committees are concerned about the costly nature of achieving the envisaged level of interoperability if online consumer services cannot transfer data in a standardised format that can be automatically interpreted.

The Committees submit that any proposed extension of the CDR should be subject to a cost-benefit analysis. If participation in the CDR framework requires significant technological capacity, small to medium enterprises may not have access to sufficient resources to develop such capacity. This may lead to heightened barriers to entry. Achieving interoperability with a high level of data security is a problem even for sophisticated organisations, as evidenced by the six month delay in implementing the Open Banking regime due to security and privacy concerns.[21]

In extending the CDR, the efficient operation of markets should not be hindered by the imposition of excessive costs (or an expectation that large costs should be expended) on companies in developing interoperability software and complying with ongoing regulatory burdens, in order to benefit from the CDR regime.[22]

[20] James Meese, Punit Jagasia and James Arvanitakis, 'Citizen or consumer? Contrasting Australia and Europe's data protection policies' (2019) 8(2) Internet Policy Review 1, 6.
[21] Australian Competition and Consumer Commission, 'Consumer Data Right timeline update' (Media Release 249/19, 20 December 2019).
[22] Australian Competition and Consumer Commission, 'Consumer Data Right Timeline Update' (Media Release 249/19, 20 December 2019).

Consumer Protection

CDR Consent

The CDR Rules require that, prior to the disclosure and use of the CDR data, consumers provide consent that is voluntary, express, informed, specific as to purpose, time-limited and easily withdrawn. [23] The Committees submit that, while the requirement of consent represents an important consumer safeguard, there is insufficient guidance about the permissible uses of the CDR data once that consent is provided. For example, a consumer may consent to their CDR data being used to determine the price of goods or services without contemplating that this may result in a relatively higher quote being issued for goods or services offered. Notwithstanding the detailed consent requirements, some consumers will not take the time to read and understand the consequences of giving consent. These consumers may be vulnerable to inappropriate product promotion and price discrimination, and therefore require the protection in a form of additional safeguards.

The Committees submit that there should be uniform terms and conditions and industry regulations regarding the CDR for the banking industry and other industries that the CDR may apply to in order to facilitate consumer understanding of the regime. According to s *56AI* of the *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, a person or a business enterprise can utilise the CDR as long as his or her data is counted as the CDR data[24] or can be reasonably identifiable.[25] The CDR data by definition in s 56AI (1) and (2) is sector-based information collected by an instrument designated sector, including other data directly or indirectly derived from that information. According to the designated sectors by the Minister,[26] consumer data includes personal data and machine-generated data. It will be difficult for consumers to understand what kind of personal data and machine-generated data that have been kept in the banking industry. This understanding is essential for taking advantage of the positive impacts data portability may have on consumer choices.

The Committees submit that regulations should be adopted prescribing uniform standard terms for CDR contracts and the technical process of transferring consumer data. Given that the collection

---

[23] *Competition and Consumer (Consumer Data Right) Rules 2020* (4 February 2020) div 4.3, r 4.9; 4.11 <https://www.accc.gov.au/system/files/CDR%20Rules%20-%20Final%20-%206%20February%202020.pdf >.
[24] Hon Josh Frydenberg MP, Treasury Laws Amendment (Consumer Data Right) Bill 2019 Explanatory Memorandum Chapter 1 1.1. < https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6281_ems_58a7c56b-36e3-4388-acf8-58455b983a76/upload_pdf/698114.pdf;fileType=application%2Fpdf >.
[25] Treasury Laws Amendment (Consumer Data Right) Bill 2019 s 56AI (3).
[26] Treasury Laws Amendment (Consumer Data Right) Bill 2019 s 56AQ.

and use of consumer data are based on contracts between a data holder and a consumer,[27] the Committees are concerned about the use of unfair contract terms. Notwithstanding the enhanced ability of the consumers to negotiate deals with the data holders due to the portability afforded by the CDR, consumers hold far less bargaining power vis-a-vis a corporation and, in the absence of unified contract terms, may have insufficient say in how their data will be used and transferred.

Inappropriate product promotion

The Committees recommend that the CDR Rules should prescribe limits to the types of products and services that may be recommended using data derived from the CDR. Inappropriate product promotion may arise, for example, in the context of a consumer applying for a personal loan using a comparison website. In this example, the Open Banking framework may permit the consumer's bank to transfer personal transaction data including payment history, salary, and spending habits. This would enable a comparison website to recommend products that are unrelated to the consumer's query, including high-interest credit cards. The consumer may be disadvantaged because the recommended products may not be suitable for the consumer's personal circumstances and financial goals.

Price discrimination

The Committees submit that the CDR may give rise to first-degree price discrimination or 'personalised pricing', which involves firms setting prices that equate to each consumer's willingness to pay for goods or services.[28] This is because the CDR data accessible through the Open Banking framework includes a consumer's transaction history, account balance, and income information.

For example, the CDR data relating to previous purchases by a consumer may be used by a comparison website to recommend personal loan products on less favourable terms than would otherwise be the case, including products that feature higher interest rates or substantial termination fees. This is because a comparison site or a firm may use the CDR data to discern the limits of a consumer's spending appetite to formulate its pricing. The foregoing use of the CDR is plainly inconsistent with the objects of promoting fairness and consumer choice[29] and would arguably result in higher consumer prices, which is contrary to the consumer-focus of the CDR[30] and should be discouraged as a matter of public policy. Further, a significant number of Australians

[27] *Competition and Consumer (Consumer Data) Rules 2019* dated 29 March 2019, r 1.8.
[28] Organisation for Economic Co-operation and Development, 'Price Discrimination' (Background Note DAF/COMP(2016)15, 29-30 November 2016) 7 <https://one.oecd.org/document/DAF/COMP(2016)15/en/pdf>.
[29] *Competition and Consumer Act 2010* (Cth) s 56AA(c).
[30] Australian Government, *Consumer Data Right Overview* (September 2019) 1 <https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf>.

fall outside the scope of protection afforded by the *Australian Consumer Law* on the basis they are insufficiently disadvantaged.[31]

Increased risk of cyber attack

The Committees submit that due to the likely increase of transfer sensitive consumer data there is a heightened risk of cyber-attacks and data abuse. Although the CDR establishes a minimum standard for privacy protection for the collection, disclosure, and use of data and imposes restrictions on the transfer of data, the holding and transferring of sensitive data, by their nature, create risks of misuse, mistake, and malware attacks.

In anticipation of this, the Committees submit that the CDR should establish minimum encryption and security measures for data holders and accredited data recipients. Furthermore, there should be regular reviews and updated standards to ensure that user data is appropriately protected.

While the auditing abilities provided for in subdivision 9.3.2 of the CDR Rules provide for some accountability in respect of data security, strong economic incentives should be in place to ensure that those dealing with consumer data appropriately protect that data. Accordingly, the Committees recommend that data holders and authorised data recipients:

a. in the event of the discovery of a breach in their data security, be under an obligation to halt any potentially at-risk services until the breach has been rectified, and report the breach to an appropriate regulatory body (with appropriate penalties to discourage the concealment of breaches); and
b. be liable to consumers in damages for any losses caused by any such data breach, including by the halting of services until the rectification of the breach.

Addressing vulnerable consumer risks

The Committees submit that although the CDR provides for increased competitiveness and transparency of financial providers, it can also serve to discriminate against vulnerable consumers. Technological access and literacy present significant disadvantages for consumers using the CDR. The Office of the Australian Information Commissioner should provide accessible educational resources to guide consumers as a first step in protecting their privacy.

[31] See *Competition and Consumer Act 2010* (Cth) sch 2 ('Australian Consumer Law') ss 21, 22; *Paciocco v Australia and New Zealand Banking Group Ltd* (2015) 236 FCR 199, 274 (Allsop CJ); *Kakavas v Crown Melbourne Ltd* (2013) 250 CLR 392, 427.

Reliable deletion and removal requests

The Committees submit that the ability for customers to request data removal and deletion from nominated data holders is an essential aspect of the CDR, which needs to be carefully monitored and enforced through reliable oversight and reporting means. This requires a combination of increased protections and rules governing data holders, efficiency in reporting and enforcing compliance, and, when necessary, penalties for non-compliance. The Committees support the enforcement of rule 4.17 of the CDR Rules when dealing with and deleting redundant CDR data.[32] Moreover, the continued use of de-identified CDR data, as determined by rule 1.17 of the CDR Rules, is reasonable in order to allow de-identified data sharing to assist consumer knowledge and product comparison.[33]

Privacy concerns

The Committees consider the current privacy regime, consisting of both industry-wide and sector-specific federal, state and territory legislation,[34] does not adequately address the potential privacy and compliance issues resulting from the CDR, for the reasons set out below.

Scope for Harm

Private entities, in gathering and processing data about an individual, may do so in an inadvertently or otherwise discriminatory manner. While the existing framework in Privacy Safeguard 11[35] considers this in the form of out of date or incomplete data, the data available to a decision matrix may result in or prefer biased or unfair outcomes for a range of other reasons, particularly in a commercial setting.

When considering that machine learning may create correlative connections which inform decision-making, it becomes important to anticipate what information and inferences should appropriately be provided to a decision-making system. Too little data, or too much data, may result in arbitrary bias which may not be immediately identifiable.

To expand on the previously discussed harm of price discrimination, by way of an example, a flight aggregator may use personal data to combine their customer's IP address with behavioural purchase information. This sets a flight price and presents it in a way which creates a unique price-

[32] *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) r 4.17.
[33] *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) r 1.17.
[34] *Federal Privacy Act 1988* (Cth); *Information Privacy Act 2014* (ACT); *Information Act 2002* (NT); *Privacy and Personal Information Protection Act 1998* (NSW), *Information Privacy Act 2009* (QLD); *Personal Information Protection Act 2004* (TAS); *Privacy and Data Protection Act 2014* (VIC). See e.g. *Telecommunications Act 1997* (Cth); *Criminal Code Act 1995* (Cth); *National Health Act 1953* (Cth); *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Workplace Surveillance Act 2005* (NSW).
[35] Competition and Consumer Act 2010 (Cth) pt IVD div 5 sub-div E s 56EN.

point for a specific consumer. This leads to greater sales and profit for the company but provides no benefit for the consumer and, likely unbeknownst to the consumer, their personal information has been used potentially to their detriment.

Perhaps of graver concern is the potential material consequences on that individual's ability to obtain essential services such as employment,[36] housing,[37] loans[38] and healthcare.[39] One adverse decision can have a flow on impact on other decisions. For example, if one entity relies on an incorrect, biased, or over-abundant data source to make an adverse decision about an individual, that decision may itself become a data point in decisions by other entities. This could in some scenarios, create a cascading series of adverse decisions for potentially essential services utilising the CDR, such as banking and other financial services.[40]

Data, and the systems which rely on data to provide services and make decisions, are inextricably intertwined. Recognising the examples of system bias in algorithms and advocating for explainability is not enough in and of itself and should not discharge the responsibility for data holders to consider, prevent and remedy potentially discriminatory outcomes.

Consumer Access

The Committees submit that systemic explainability should act as a *minimum* standard, particularly given the increasing complexity of data practices. In AI decision systems, for example, technical information used in the development of the system (such as the model, "values and constraints that shape…conceptualization", how these values shape the machine learning, and "how outputs…inform final decisions")[41] may be as essential to understanding the relationship between decisions and data. When we can see the usefulness of this kind of information for vulnerable consumers, it is clear that explainability is not a panacea for privacy concerns in complex digital

[36] Alexander Tischbirek, 'Artificial Intelligence and Discrimination: Discriminating Against Discriminatory Systems' in Thomas Wischmeyer and Timo Rademacher (ed), Regulating Artificial Intelligence (Springer, 2020) 103, 112 -113 [25]-[26].
[37] Bryan Casey, Ashkon Farhangi, and Roland Vogt, 'Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise' (2019) 34(1) Berkeley Technology Law Journal 143, 147.
[38] Andrew Selbst and Solon Barocas, 'The Intuitive Appeal of Explainable Machines' (2018) 87(3) Fordham Law Review 1085, 1102-1104; Christian Ernst, 'Artificial Intelligence and Autonomy: Self Determination in the Age of Automated Systems' in Thomas Wischmeyer and Timo Rademacher (ed), Regulating Artificial Intelligence (Springer, 2020) 53, 55 [4]-[5].
[39] Fruzsina Molnar-Gabor, 'Artificial Intelligence in Healthcare: Doctors, Patients and Liabilities' in Thomas Wischmeyer and Timo Rademacher (ed), Regulating Artificial Intelligence (Springer, 2020) 337, 337.
[40] For example, flow on effects of a creditworthiness decision: Andrew Selbst and Solon Barocas, 'The Intuitive Appeal of Explainable Machines' (2018) 87(3) Fordham Law Review 1085, 1102-1104.
[41] Andrew Selbst and Solon Barocas, 'The Intuitive Appeal of Explainable Machines' (2018) 87(3) *Fordham Law Review* 1085, 1130.

spaces.

The impact of inadvertent or residual disclosures about third parties should be carefully considered from a privacy perspective. The Committees acknowledge the role of Privacy Safeguard 4[42] and Privacy Principle 4[43] in placing the onus on the recipient of unsolicited data to destroy it, however, it is notable that there are no recorded privacy determinations to date which address Principle 4.[44]

One example is residual or inadvertent disclosure is that of children, whose data is largely under the control of their guardian until adolescence and adulthood, and whose information may be easily discernible from that of their guardian, or disclosed by association. While the use of a child's information may be captured by Privacy Safeguard 6[45] (and Privacy Principle 6)[46] there are exceptions to the application of the Safeguard in uses for direct marketing, and likely parental consent would be sufficient in a practical sense. Given the highlighted issues of complex harm, and challenges to the explainability of the systems which operate on such data, it remains a concern if inadvertent disclosure measures meet the needs of vulnerable users.

The Committees further submit that the ability of the CDR to positively impact consumers is reliant on consumers' willingness to engage with their rights, and being able to hold data controllers to account and demand a high level of security in order to feel secure. Currently, research shows a lack of engagement with the existing framework.[47] This is in the context of consumers developing a deep mistrust of online platforms following data scandals such as Facebook/Cambridge Analytica,[48] and HealthEngine.[49] The Committees recommend that an educational campaign be undertaken to engage consumers in discussions about the CDR through the holding of online and in-person seminars and/or workshops and disseminating information about the use and operation of the CDR online.

---

[42] *Competition and Consumer Act 2010* (Cth) pt IVD div 5 sub-div C s 56EG.
[43] *Privacy Act 1988* Sch 1, Pt 1.
[44] 'Privacy Determinations,' *Australian Government – Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/privacy/privacy-decisions/privacy-determinations/>.
[45] *Competition and Consumer Act 2010* (Cth) pt IVD div 5 sub-div D s 56EI.
[46] *Privacy Act 1988* (Cth) sch 1 pt 3 s 6.
[47] James Meese et al., 'Citizen or consumer? Constructing Australia and Europe's data protection polices' (2019) 8(2) *Internet Policy Review: Journal on Internet Regulation* 1, 6; Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey* (Report, 15 May 2017) 15.
[48] 'Cambridge Analytica Harvested Data from More than 87 Million Facebook Users, Whistleblower Says', *ABC News* (online, 18 April 2018) <https://www.abc.net.au/news/2018-04-18/cambridge-analytica-employee-testifies-before-uk-committee/9670192>.
[49] Pat McGrath, 'HealthEngine, medical booking app, facing multi-million-dollar fines for selling patient data', *ABC News* (online, 8 August 2019) <https://www.abc.net.au/news/2019-08-08/healthengine-facing-massive-fine-after-abc-investigation/11394564>.

This would clarify confusion regarding rights and expectations flowing from the new right, and encourage consumers to engage with their rights and make informed decisions under the CDR framework. The Committees further propose that extending this engagement to providing business with industry specific guidance on the necessary changes to ensure their data practices are compliant may be beneficial. This is particularly so for small to medium enterprises who lack the resources to ensure compliance without some additional assistance.

The Committees recommend that accredited data recipients be required to disclose the CDR data relating to the consumer that is already in its possession, in addition to any other data relating to the consumer that it intends to combine with the CDR data. This would ensure that further consideration is given to protections designed 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.

Finally, the Committees recognise that education designed to increase consumer awareness of the CDR plays a critical role in achieving the privacy outcomes targeted for the Consumer Data Right Safeguards framework. Further, when considering the complexity of the current interaction of legislation surrounding privacy, education may not be enough particularly for vulnerable consumers with limited access to legal advice. The Committees submit that an unambiguous identification of enforceable rights with respect to the use of their own CDR data is essential for realising privacy outcomes for consumers under the current system. Ambiguity is likely to reduce the value and bargaining power that a consumer could otherwise derive from the CDR.

Redress and Remedies

The Committees submit that the complexities of the current regime may hinder consumer trust because of the insufficient understanding of how consumer rights are protected. In the digital context, the privacy regime is further complicated by a regulatory level relating to consumer data practices, where the Office of the Australian Information Commissioner (OAIC) and Australian Competition and Consumer Commission are charged with ensuring compliance over particular conduct.

The Committees support and recommend the inclusion of private remedies for individuals (for example privately-recoverable pecuniary penalties), in addition to the ability to complain o the relevant enforcement agency, in respect of the misuse or inappropriate disclosure of CDR data. The Committees consider it important to provide aggrieved consumers and individuals who have suffered an alleged breach of their privacy due to non-compliance with the CDR with practical avenues to seek relief independent of enforcement agencies. In the context of the growing importance of consumer data and future CDR participants increasingly relying on data relating to

individuals to make decisions which affect them, providing consumers with private remedies is important in accounting for the significant impact incorrect or unauthorised data can have upon an individual's life.

Further, providing individuals this right reduces the burden on enforcement agencies, thereby enabling them to focus on the most egregious cases, and the most vulnerable consumers who may be unable to engage with private systems of redress. This risk of litigation would also further incentivise CDR participants to comply with their obligations under the Consumer Data Right Safeguards framework.[50]

Formalisation of Consumer Protections

The Committees are of the view that 'de-identification' is a critical aspect of the CDR and should be contained within Parliament enacted statute rather than left to outside frameworks. The control mechanism of deletion and 'de-identification' enable consumers to protect their privacy from the risk of misuse. The importance of deletion has already been discussed above, however, unless de-identification is defined clearly in legislation, the references to it may be highly problematic.

Acknowledging the existing Data-61 Framework,[51] and the complexity of the decision of de-identification, the Committees note that the conventional approach of removing identifiers such as name, address, and date of birth from collected data which contains or concerns personal 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. 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 as machine learning technology continues to develop. The complexity of these processes should be weighed against the barriers to consumer confidence that a lack of transparency or certainty may entail.

The Committees recommend that the definition of de-identification should be extended to require that all copies of the redundant data be permanently transformed into a state from which they can no longer be used to identify the consumer to whom it relates. That is, they should be anonymized to an extent that is impossible to be able to re-identify the individual. Certain technologies and programs could assist with this, such as *k*-anonymity. This should consider (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.

---

[50] *Competition and Consumer Act 2010* (Cth) pt IVD div 5; OAIC, *Consumer Data Right Privacy Safety Guidelines*, 2020 < https://www.oaic.gov.au/assets/consumer-data-right/cdr-privacy-safeguard-guidelines-february-2020.pdf>.

[51] [16] Christine M O'Keefe et al, 'The De-Identification Decision-Making Framework' (CSIRO Report EP173122 and EP175702, CSIRO, September 2017) < https://data61.csiro.au/en/Our-Research/Our-Work/Safety-and-Security/Privacy-Preservation/De-identification-Decision-Making-Framework>.

The Committees want to emphasise these considerations may be of greater significance in the context of artificial intelligence and machine learning systems. The requirements to delete or de-identify data held may be complicated where an algorithm has already relied on that information as a data point. This raises the possibility that the data is discernible from the algorithm itself, and extremely challenging to 'destroy' data as understood by the requirements of Privacy Safeguard 12.[52] This risk may be compounded where the decision made has created a negative or discriminatory outcome based on the data which is indelibly embedded within a complex decision-making program.

[52] *Competition and Consumer Act 2010* (Cth) pt IVD div 5 sub-div E s 56EO.

THE LAW SOCIETY OF NEW SOUTH WALES
YOUNG LAWYERS

Concluding Comments

NSW Young Lawyers and the Committees thank you for the opportunity to make this submission. If you have any queries or require further submissions please contact the undersigned at your convenience.

Contact:

David Edney

President

NSW Young Lawyers

Email: president@younglawyers.com.au

Alternate Contact:

Olga Kubyk

Chair

NSW Young Lawyers Business Law Committee

Email: olga.kubyk@younglawyers.com.au

Alternate Contact:

Ashleigh Fehrenbach

Chair

NSW Young Lawyers Communications, Entertainment and Technology Committee

Email: ashleigh.fehrenbach@younglawyers.com.au