AUSCL

AUSTRALIAN SOCIETY FOR
COMPUTERS & LAW

2 September 2021

Strategic Assessment Team

Consumer Data Right Division
The Treasury
Langton Crescent
PARKES ACT 2600

By email: data@treasury.gov.au

Submission to the Consumer Data Right - strategic assessment

The Australian Society for Computers and Law (AUSCL) is an interdisciplinary network of professionals and academics focussed on issues arising at the intersection of technology, law, and society. It is a non-profit, registered Australian charity with a charter to advance education and policy development. AUSCL was officially launched in July 2020, but its member State societies were formed as early as 1981. AUSCL provides a forum for learned discussion and debate through its Policy Lab, Working Groups and Events Program attracting support and engagement across Australia and globally.

This submission

Thank you for the opportunity to contribute to this Strategic Assessment process. Comments in this submission are confined to questions 8-12. It is acknowledged that in undertaking the process of rolling out CDR economy-wide, the Government will need to contend with many complex issues that take account of the interests of stakeholders across a broad range of sectors, and complex and evolving policy matters.

To obtain best value from this process, this submission recommends further consideration of consumer protection, privacy, intellectual property and cybersecurity matters that go beyond the immediate focus of CDR itself (as acknowledged by the discussion paper). This submission also recommends further consideration of the potential affordance of alternative approaches to constructing appropriate regulatory guidance that might provide. In doing so, this submission does not purport to provide a simple and complete solution to what is necessarily a complex problem space, but rather to stimulate broader thinking about what might be possible, in order that the benefits of CDR are more likely to be obtained, and at a lower risk to the consumer

(whose broader interests should naturally be the prime focus of this regime). A key focus of this submission is around the final strategic assessment criterion, namely "safer and more secure data sharing practices".

General Comments on CDR Strategic Vision and framing of the issues

Before the specific nominated questions are addressed, first some comments on the Strategic Vision and framing of the CDR regime as set down in the consultation paper:

- A proper "'wrap-around' view of a consumer's data touchpoints"[1]requires consideration of people's activities, generation use and sharing of data beyond an immediate transactional focus. Events of recent years, from Cambridge Analytica and beyond, are ample demonstration of the extent to which consumer data can be manipulated and used in pernicious and malicious ways that extend beyond consumer and commercial areas into threats to social cohesion, political systems and even national security.
- The Strategic Vision paints a picture of "CDR puts consumers in the driver's seat to use data collected on them, for their own benefit, based on their specific circumstances", and says data will be transformed "from being an inaccessible resource used by businesses for profit, to an invaluable tool that consumers can control and benefit from as well". However, an individual necessarily only has a view of their own data, they do not have the benefit of an aggregated access to data in the same way that a business does. The reality is that CDR as currently framed will remain primarily a tool for business, not a tool for consumers. Consumers might be forgiven for feeling more like tradeable data objects than empowered subjects. With respect, consultations on CDR to date seem largely directed to the interests of current and prospective service providers around functional standards protocols and regulations and industry facing. The consultation does not feel primarily consumer oriented and consumer/citizen voices seem to have been a relatively small component of the overall discussion to date. This is problematic in the context of properly realising the strategic assessment's goals of consumer centricity.
- Overall, the CDR regime posits a construct of person as consumer and consumer as a rational decision maker in an improved (albeit imperfect) new information market enabled by CDR. It conceives of consumers as having clear preferences and a defined risk appetite. But consumer decisions – as recognised by intellectual property and consumer laws and the harms they target – are often

[1] Discussion Paper (DP) [8]

made in a rush for convenience based on factors such as brand trust and without regard to more detailed information, even if on offer. An example may be seen in the context of digital environments where terms and conditions of engagement with many services may be seen as egregious in the extent of data sharing and profiling that they permit – most consumers blithely "accept" terms without ever reading them or understanding their import. This can lead to direct consumer harm rather than benefit: for example in areas such as differential pricing.[2]

- The Strategic Assessment invites "a more conceptual approach to CDR expansion which focuses on areas and phases in a consumers' life that could be improved through access to datasets relevant to a consumer action or event, and not necessarily linked to one sector". This is consistent with some of the discussion above. The Strategic Assessment also notes that this broader focus "will likely transcend the boundaries of a particular sector or sector-specific dataset and involve a range of data held by different data holders".[3] This is consistent with some of the suggestions below that invite contemplation of alternative approaches to economy-wide roll out that focus less on the individual features of data in particular sectors, but rather have a greater focus on the "rolled up" effect on the consumer and are addressed on a principle basis to counter potential harm.

Q8: Are there sectors with competition issues which would more readily benefit from reductions of data-related barriers? For example, to facilitate providers responding to competitive pressure by improving products and services, new market entries or increased transparency.

Digital Platforms - in particular Social media digital platforms - probably have the largest volume of consumer data. They also have fairly high barriers to data-sharing, notwithstanding that they have some policies and processes to permit this within limited bounds.[4] Constraints around movement of this data to other platforms

---

[2] See eg Paterson, Jeannie; Bush, Gabby; Miller, Tim --- "Transparency to contest differential pricing" [2021] ANZCompuLawJl 13; (2021) 93 Computers & Law 49 http://classic.austlii.edu.au/au/journals/ANZCompuLawJl/2021/13.htm : "Although many consumers are yielding personal data that fuels these processes, it is not clear that they understand the consequences of such uses. Further, the incidence of differential pricing is difficult to discover. Such conduct runs counter to the common emphasis in formulations of standards for ethics in the use of artificial intelligence, which emphasise transparency and opportunities to contest adverse decisions"

[3] DP [15]

[4] For instance, while Facebook has recently improved some limited functionality to export some information, it does not provide full data portability and indicates it will not do so without regulation - see eg <https://about.fb.com/news/2021/04/transfer-your-facebook-posts-and-notes-with-our-expanded-data-portability-tool/>

reinforces market network effects and natural inertia to produce the market dominance that we see from the likes of Facebook. This sector would benefit from reduction in data related barriers that readily enabled fairly frictionless and transparent inter-operability, permitting other providers to enter the market in various niches.[5]

In addition much of this data is inherently social and community oriented, so the constraints around it and the effective "lock in" that can induce can have many problematic impacts. The recent problems experienced when Facebook temporarily shut down access to 'news' in Australia in the context of the Government's proposals to regulate designated digital platforms through the News Media Bargaining Code are testimony to that.[6] This can have safety and political impacts that extend beyond the commercial.[7]

In making these comments, it is recognised that Australia's power to effectively regulate for such standards on its own may be somewhat limited given the transborder nature of most of the digital platforms, and the fact that none of the major platforms have Australia as their home jurisdiction. Nonetheless, there is clearly a growing level of cross border regulatory co-operation in related fields,[8] so these matters bear further investigation and progress, notwithstanding that those sectors may not be as immediately amenable to regulation as the sectors prioritised to date, where due to the nature of the composition of the sector many of the major Australian providers are domestically based.

---

[5] Instead the status quo sees major platform providers such as Facebook shutting out competitors - see eg <https://www.afr.com/technology/aussie-ipo-hopeful-in-limbo-after-sudden-facebook-ban-20190901-p52mxb>

[6] See eg ABC, "These graphs tell the story of the Facebook news ban — and what happened after" <https://www.abc.net.au/news/science/2021-03-03/facebook-news-ban-australian-publisher-page-views-rebound/13206616>; Josh Taylor "Facebook's botched Australia news ban hits health departments, charities and its own pages" (Guardian) <https://www.theguardian.com/technology/2021/feb/18/facebook-blocks-health-departments-charities-and-its-own-pages-in-botched-australia-news-ban>.

[7] See eg BBC "Cambridge Analytica: The story so far" available at <https://www.bbc.com/news/technology-43465968>

[8] In respect of ACCC there has been international co-operation at least between the relevant Australian and UK authorities on digital platform issues – see eg Australian Competition and Consumer Commission, Digital Platform Inquiry (Final Report, 26 July 2019) <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report>; Competition and Markets Authority, Online platforms and digital advertising Market study (Interim report, 18 December 2019). In respect of ASIC, there is international co-operation through the Global Financial Innovation Network of regulators – see < https://www.thegfin.com/>. ASIC also has designated "Strategic Intelligence" staff. These developments pre-dated the pandemic by two years (for example the), but in a webinar ASIC confirmed in response to a question that the pandemic has accelerated this co-operation - ASIC Regtech Liaison Forum 7 August 2020. ASIC noted a clear increase in discussion around regtech, supervisory tech and standards to promote use of international datasets.

However, prioritising action on digital platforms could work hand in glove with other approaches (e.g. ACCC work on digital platforms from a competition perspective) in order to create a more level playing field and a fairer environment for consumers.

Another potential area where data issues may be relevant for individuals and business (dependent on how farms are structured), is in the agricultural environment. Here John Deere and other product and service providers are increasingly seeking to arrogate control over farm data gathered by their systems.[9]

Q9: Which sector market's efficiency could be improved by making consumer and product data readily transferable to other providers? Are there sectors where there is currently a high transaction cost to release and disperse this data that the CDR could address?

If consumer and product data becomes readily transferable, markets such as digital platforms, telecommunication services (internet and phone providers), insurance, banking and retail loyalty programs and other everyday service providers' efficiency could be improved.

Markets using non-digital products or using highly specialised products, such as healthcare and medical, will be subject to a higher transaction cost due to the manual costs involved and the difficulty to generate data from specialised platforms. Again, Digital Platforms and Agricultural Product/Service data are suggested as relevant areas of focus. There may be some cross linkages to government responses to other contemporary issues such as intellectual property reform and 'right to repair' approaches.[10]

However, in all these areas the concerns discussed elsewhere in this submission hold.

Q10: Are there other steps we could take to strengthen or develop the CDR regime to enhance the economy-wide roll-out?

Economy wide v sector by sector: room for an alternative principles based approach?

---

[9] See eg Horton, Thomas Jeffrey and Kirchmeier, Dylan, John Deere's Attempted Monopolization of Equipment Repair, and the Digital Agricultural Data Market - Who Will Stand Up for American Farmers? (January 13, 2020). CPI Antitrust Chronicle, Jan. 2020, at 2, available at <https://ssrn.com/abstract=3541149>.

[10] See eg <https://www.pc.gov.au/inquiries/current/repair#report>.

There will be difficult tensions to navigate in moving towards an economy wide rollout. Prima facie, the more variable the rules around particular sectors are, the more uncertainties and difficulties will be created at the interface between sectors. Crisp boundaries between sectors may prove increasingly difficult to maintain in the face of new intermixed business models that span multiple sectors. Regulatory design and targeting therefore becomes a very important and vexed issue, especially to the extent that there may be legitimate and important differences in the context of a given sector.

One small but common example of this can be seen in regulatory targeting matters that emerge when new technologies or business models evade prior regulatory structures that control 'equivalent' services because of definitional constraints.[11] It is submitted that trying to cover the field effectively in a way that is detailed and robust and 'neutral' to shifts in technology and business models is extremely fraught.

Therefore, it may be that a new approach is needed that focuses less on the features of a particular sector or data set, and more on the impact of the scale and combination of different datasets, potentially viewed through the lens of the net interests of the citizen/consumer. If such an approach was taken, it is likely it would need to be more principles based as creating detailed guidance around such matters – even if assisted by an algorithmic/regtech implementation - would be very challenging. While some may criticise principles based approaches for providing insufficiently nuanced guidance, the reality is that principles based approaches to important issues are very successful and important parts of our governance structures in adjacent fields of law.[12]

If we focus less on the data itself and more on the integrated impact of the aggregation, manipulation and use of that data by individuals or organisations then we may be closer to a workable solution approach. This could also enable particular harms to be the focus of the approach – for example: disinformation especially where coupled to other already identified harms (discrimination, blackmail, etc). Properly articulating this approach in the scope of this submission is not possible – it is offered as an alternative if divergent solution concept. It could include setting new standards through mechanisms such as the Australian Consumer Law putting obligations on companies not to engage in particular data practices that are likely to have adverse consumer impacts.

The importance of trust: coupling CDR to improvements in privacy and cybersecurity measures and obligations

As the discussion paper highlights, privacy and security considerations are key to user safety and trust. The discussion paper states that the assessment "provides the

[11] for example, consider mesh networks substituting for telecommunications services, or Afterpay substituting for credit services.
[12] for example s.18 of the Australian Consumer Law.

opportunity to step-back and consider implementation having regard to key phases, decision points and life events for a consumer where improved access to data could reduce time, hassle and cost and support consumers make more informed decisions". But there are more issues at stake than reduction or time hassle and cost in transactional environments. And there are many situations where simply enabling 'more' informed decisions is necessary but insufficient: where broader harms or pernicious or malicious behaviours need to be taken into account. The new structures being developed by the system are also open to abuse. Risks include leakage of sensitive personal information, identity theft, exposure of information to small entities without the security and prudential frameworks and cultures that older institutions have developed. Even the very inefficiencies and obscurities of the current silos of information, problematic from the perspective of competition as they undoubtedly are, act as a form of brake on abuses that could run rampant in an environment where data was much more accessible and portable.

The technology sector is belatedly recognising – including at very senior levels - that its longer term viability requires a more concerted focus on privacy and trust:

> "Sure, raking in all this personal user data is convenient. Lead is also a great ingredient in paint: It's anticorrosive, it helps coats dry faster, and it increases moisture resistance. But we outlawed lead in paint anyway, for reasons that now seem chillingly obvious. We can do the same for data surveillance. Because of course it's not too late. Seat belts became mandatory in the US in 1968, many decades after cars became an integral part of life. Airbags and emission controls didn't develop overnight either—or without prodding. Regulation forced the car industry to innovate. It developed safer and cleaner cars, and remained quite profitable."[13]

See also Tim Cook (Apple CEO): ''People know that the web has become this surveillance tool in all too many cases, and that the building of detailed profiles on people has gone well beyond any kind of reasonable thing…It's the detailed profile that enables people to pit one group against the other."[14]

So, there is a manifest need to ensure that the design and rollout of the CDR goes hand in glove with appropriate progress on other matters such as privacy and cybersecurity in particular, as the discussion paper identifies, as these matters are critical to trust and protection. There have been a great number of prior recommendations for improvement of Australia's standards in these areas.[15]

---

[13] Jeffrey Hammerbacher "YES, BIG PLATFORMS COULD CHANGE THEIR BUSINESS MODELS" Wired 17/12/18 available at <https://www.wired.com/story/big-platforms-could-change-business-models/>.

[14] quoted in Matthew Drummond "Apple to the core, Cook says trust is key to tech's success" Australian Financial Review 20 August 2021 [2].

[15] ACCC Digital Platforms Inquiry FInal Report <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report> made recommendations for the reform of the Privacy Act 1988 (Cth); ALRC, Serious Invasions of Privacy in the Digital Era (ALRC Report 123)

It is submitted that current systems of protection, including the cybersecurity standards within the CDR regime itself, are insufficient, especially when viewed through the prism of emerging and likely threats. Higher standards need to be set. Standards around ADRs in particular are, with respect, not that strong. This will not be addressed properly simply by improving redress avenues for those who suffer some breach. There are many data breaches that are very difficult to adequately address in that way, as once for instance someone's biometric data is breached, they are in a very problematic position as they cannot readily change the source of that data – it is not possible to change one's face or gait in the way one might get a new licence.

It is also submitted that other approaches that the government is exploring at the moment to assisting consumers with the complex issues around cybersecurity – such as certificates around ratings and expiry dates, are also problematic and do not take account of either the complexity of even common places such as IT environments, or the usual norms of consumer behaviour. Consumers are simply not in a position to sensibly self-protect. Rather those companies and organisations with the resources and the knowledge to take protective action must be charged with an active responsibility to do this. Again this is likely to require a principle based reform approach – which might in part be addressed by new provisions in the Australian Consumer Law setting baseline obligations and guarantees in these areas.

It is also suggested that one aspect of the approach could be to consider the level of granularity of the data access that is provided. It is suggested that for many purposes, in order to achieve the desired product/service fit to consumer needs, alternative providers or intermediaries probably do not require access to full granularity of data. Rather they may be able to match on the basis of a higher level of generality (we see this type of approach emerging already in the market - for example, Google's 'federated learning of cohorts' model). It is submitted that there should be a principle of organisations only accessing the minimum subset or abstract profile they need. Businesses may need a richer picture but not a complete one. And if there are approaches that are consistent with federated data principles for protecting data (that do not require data to be moved) then they should be adopted. However it is important to stress that this on its own is insufficient to protect consumers against harm, for reasons discussed elsewhere including below in relation to the contextual nature of sensitive information and the power of inferencing.

Further, it is strongly submitted that there are longer term potential benefits - including to industry - of having a more robust level of protection of consumer interests on these matters. It is also submitted that we need new approaches to

privacy impact assessments, that do not look at privacy in a narrow sector by sector dataset oriented fashion – but rather take a more holistic consumer harm perspective, integrated across different domains. For this is where we have seen the problems emerge.

While beyond the immediate scope of this review, it is noted that the same issues apply in other fields such as government provision of access to public sector data to the private sector under the auspices of the *Data Availability and Transparency Bill 2020* [Provisions] and *Data Availability and Transparency (Consequential Amendments) Bill 2020* [Provisions] . This submission notes the recommendation from the Senate Finance and Public Administration Legislation Committee on these bills, which called for further assurances and consideration in relation to security and privacy matters, inducing "particularly in relation to the de-identifying of personal data that may be provided under the bill's data-sharing scheme".[16]

Q11: Are there any datasets or kinds of data that may or may not be suitable for Consumer Data Right designation (e.g. due to privacy concerns)? Why?

There are some obvious categories of data, such as health data and other information that might fall with "sensitive" categories in the current framing of the *Privacy Act 1988* (Cth). There are also many analyses of examples of other datasets (such as telecommunications datasets) that point clearly to the vast array of inferences that can be derived even from metadata.[17]

However, it is suggested that trying to quarantine by data type may be increasingly problematic for a range of reasons. This includes the proliferation of new technologies and business models discussed above, which may generate new types of data that may be viewed as sensitive. It also relates to the broader issue that the sensitivity may arise from the aggregation of otherwise innocent looking non sensitive data. Sensitivity is complex and contextual. As the Treasury paper notes "consumers may have concerns about the sharing of data with particular businesses, or the sharing of particular types of data, via the CDR. ***While certain kinds of data may be considered sensitive, such as location data or internet browsing data, data***

---

[16] Commonwealth Senate Finance and Public Administration Legislation Committee Report on Data Availability and Transparency Bill 2020 [Provisions] and Data Availability and Transparency (Consequential Amendments) Bill 2020 [Provisions] <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/DataTransparency> [5.189 - recommendation 3]

[17] See eg <https://www.abc.net.au/news/2015-08-16/metadata-retention-privacy-phone-will-ockenden/6694152?nw=0>; <https://www.abc.net.au/news/2015-08-24/metadata-what-you-found-will-ockenden/6703626?nw=0>

may also become sensitive when combined with other datasets." (emphasis supplied)

This is also important to consider in relation to measures proposed as 'solutions' to sensitivity (including in legislation) – such as "de-identification". This can pay insufficient regard to the fact that re-identification is in many cases easier than de-identification, especially where many different data sets including non-sensitive information can be cross referenced and inferences drawn.[18]

Again this points to a different approach - as discussed above - that looks more at the aggregation, synthesis and purpose of use of the data rather than the data per se.

Q12: Are there global trends or good examples internationally of where consumer data is being used to drive better consumer and/or social outcomes? How has this informed that jurisdiction's approach to rolling out comparable data regimes?

It is suggested that in the course of this strategic assessment the impact and importance of international standards is very important. Take for example the impact of the EU's General Data Protection Regulation. This has had a 'race to the top' impact on some data sharing standards and practices internationally, given the extent of transborder reach of internet data sharing.

However, positive social outcomes can only be achieved if the security of consumer data can be ensured and sufficient governance and controls are in place to govern how consumer data will be used or on-shared.

Consider also the difficulties that Australia potentially faces in some other unrelated fields – for example in relation to climate change and carbon policy, where if it fails to at least match international standards it may be subject in the future to tariff and non tariff barriers.[19] These factors point to the difficulties that may be faced if Australia adopts a policy approach in this CDR field that may be viewed as failing to at least match standards in equivalent regulatory frameworks elsewhere, and is an argument

---

[18] See eg "The simple process of re-identifying patients in public health records" <https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records>; See also Y. J. Lee and K. H. Lee, "Re-identification of medical records by optimum quasi-identifiers," *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017, pp. 428-435, doi: 10.23919/ICACT.2017.7890125.

[19] In a recent webinar (ASIC Regtech Liaison Forum 7 August 2020) DFAT discussed its international engagement activities directed at ensuring appropriate international data trading arrangements. DFAT were asked whether they saw EU data protection settings and trends as a barrier to digital trade. The response was that the question is very much "alive" and that companies had raised cost and compliance concerns to DFAT.

against favouring an approach that may be seen superficially as attractive to business because it is privacy or consumer protection “lite”. Any gains from such an approach may be short lived.

Consultation

Please contact us if you would like to discuss any aspect of this submission either in person or as a round table discussion.

Yours sincerely,

Marina Yastreboff

President

Australian Society for Computers & Law

With thanks to our authors:

Robert Chalmers, Lecturer, Flinders University
(this contribution is made in a personal academic capacity and does not necessarily represent the views of Flinders University as an institution)

Shengshi Zhao, Director, Sentre Consulting

(this contribution is made in a personal capacity and does not necessarily represent the views of the author’s employer, clients or workplace)