

T: 03 9607 9311

E: [techandprivacy@liv.asn.au](mailto:techandprivacy@liv.asn.au)

27 April 2020

Secretariat  
The Treasury  
Langton Crescent  
Parkes ACT 2600

By email only to: [data@treasury.gov.au](mailto:data@treasury.gov.au)

Dear Mr Farrell,

### **Inquiry into Future Directions for the Consumer Data Right**

The Law Institute of Victoria (**'LIV'**) welcomes the opportunity to respond to the Treasury's Inquiry into Future Directions for the Consumer Data Right (**'the Inquiry'**). The LIV recognises and supports the objectives to provide greater consumer choice and foster market competition, however notes the CDR regime must be mindful of the delicate balance between consumer privacy, genuine consumer choice, compliance costs and the enhancement of competition and innovation. The LIV seeks to voice its concerns and provide guidance with this balance in mind.

#### **1. Expansion of 'read' access to 'write' access**

The current 'read' access provided with the Consumer Data Right (**'CDR'**) allows the sharing of CDR data with accredited third parties with the consent of the consumer. This is largely, although not exclusively, done through application programming interface (**'API'**) implemented by data holders. This development has granted customers better access to their data, which in turn encourages competition between service providers and lowers prices for consumers. The ability to 'monetise' data can also encourage innovation and the establishment of new services and offerings, which can in turn create benefits for consumers and the economy at large.

However, the LIV notes the CDR regime has considerable privacy implications. Currently, there are no tiers of accredited third parties. This means that were a customer to consent to a third party receiving their data for a specific reason, the third party would receive all of their data regardless of whether

they required it for the purposes for which the customer consented. Notably, this practice would be inconsistent with the data minimisation principle,<sup>1</sup> which dictates that an accredited person may only collect data in order to provide goods or services in accordance with a request from a CDR consumer.<sup>2</sup> Data that has ‘no bearing on the...delivery of service’ would be in breach of this principle, where the Office of the Australian Information Commissioner (**‘OAIC’**) requires collection of data to be ‘reasonably needed’ to provide goods or services.<sup>3</sup> The LIV considers the absence of a tiered system of accredited third parties to pose a substantial risk for abuse and an impediment to protecting the privacy of consumers. In the CDR Rules outline, this has been flagged as something that requires adjustment once the CDR is expanded. The LIV considers this to be of vital importance.

To expand the CDR to include ‘write access’, the European Union’s Payment Service Directive II (**‘PSD2’**), implemented under UK’s Open Banking regime, should be considered. The PSD2 enforced a similar concept, offering two streams for banks pursuant to the Open Banking concept – either banks had to establish a separate API for accredited third parties or allow these parties to use the same interface as customers. This could be emulated in Australia; however, the security risk of APIs would need to be weighed against their effectiveness for this purpose, as such access provides an additional way for fraudulent actors to access customer information.<sup>4</sup>

### Interoperability

Europe’s General Data Privacy Regulation has declared data portability—allowing users to take their data and move it to a different platform—as a basic right for all European Citizens. It recognises that free portability of personal data can both ‘enhance controllership of individuals on their own data’,<sup>5</sup> and also foster competition of digital services. Without interoperability ‘across platforms or services’,

<sup>1</sup> Australian Competition and Consumer Commission, ‘CDR Rules Outline’ (Web Page, January 2019) <<https://www.accc.gov.au/system/files/CDR-Rules-Outline-corrected-version-Jan-2019.pdf>> [7.5].

<sup>2</sup> Competition and Consumer (Consumer Data Right) Rules 2019, r 1.8.

<sup>3</sup> Ibid. r 4.11(3)(c)(i).

<sup>4</sup> Julian Lincoln, David Ryan and Audrey Vong, ‘Consumer Data Right 2020 Update’ Herbert Smith Freehills (Web Page, 20 February 2020) <<https://www.herbertsmithfreehills.com/latest-thinking/consumer-data-right-2020-update>>.

<sup>5</sup> Paul De Hert et al, ‘The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services’ (2018) 34(2) Computer Law & Security Review, 193.

effective enforcement of this right is challenging.<sup>6</sup> Yet increased data portability, where one person's data is moved to another system, creates security risks that may outweigh the portability benefits.<sup>7</sup> With different governance and privacy protections existing within Australia's privacy regime and between providers, this could have unintended consequences on consumer privacy.

For example, the ACCC itself delayed the launch of the Open Banking regime, citing the complexity of privacy and security arrangements in the finance sector. The CDR Rules outline makes specific mention to the added information security risks associated with consumers enforcing the use of APIs for the 'read' access function.<sup>8</sup> This would need to be addressed for 'write' access, as this would pose a greater risk with the additional influence provided to accredited third parties. Moreover, the LIV suggests that in addition to read/write access should be the ability to insist on deletion akin to those rights under the EU General Data Protection Regulation ('GDPR's') right to erasure.<sup>9</sup> As data can often be interlinked or inseparable, there is a need to balance what might be one person's right to their data with another person's right for that data to be erased.<sup>10</sup>

### Balancing liability

Focusing on the four principles set out by the Treasury (be consumer focussed; encourage competition; create opportunities; be efficient and fair), robust protections are required to protect consumer's privacy and data from abuse, fraud, and criminal enterprises.

Examining who is better placed to ensure consumer protections between banks and third-party

<sup>6</sup> Recital 68 of the General Data Protection Regulation states that data controllers 'should be encouraged to develop interoperable formats that enable data portability'.

<sup>7</sup> Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72(2) Maryland Law Review 350.

<sup>8</sup> Australian Competition and Consumer Commission, 'CDR Rules Outline' (Web Page, January 2019) Outline (n1) [1.4] <<https://www.accc.gov.au/system/files/CDR-Rules-Outline-corrected-version-Jan-2019.pdf>>.

<sup>9</sup> EU General Data Protection Regulation, art 17.

<sup>10</sup> Wenlong Li, 'A Tale of Two Rights: Exploring the Potential Conflict between Right to Data Portability and Right to be Forgotten under the General Data Protection Regulation' (2018) International Data Privacy Law 8(4) 309-317.

providers, the banks are financially larger and have the knowledge regarding the consumer data they hold. However, banks do not have a financial incentive to create the robust systems required to secure the data transferred and are acting at the direction of the law, while the third-party providers hold a financial incentive. Importantly the law's goal is to create new opportunities for new entrants and start-ups for the purposes of innovation and competition. To be efficient and fair, banks as the more resourced parties, financially and with personnel, should be equally liable with the third-party providers to establish the technological systems and processes necessary to ensure consumer's data and privacy are protected when being transferred between (read and write access) the banks and the third-party providers.

## 2. Addressing information asymmetry and consumer knowledge

We recommend the following to ensure that the CDR develops in a manner that is ethical, fair, inclusive of consumer needs, and socially beneficial. This should recognise the knowledge and accessibility challenges for consumers. A survey conducted by Accenture found that the majority (53 per cent) of Australian consumers do not understand the potential benefits of Open Banking enough to grant third-party providers access to their data.<sup>11</sup> Wider consumer education is needed to circumvent disproportionality in the exercise and protection of this right.

Given the accessibility hurdles in asserting the CDR, the LIV suggests greater emphasis on the protection of personal data as the primary aim behind expanding the CDR, rather than a singular focus on facilitating data flows across markets and competition. For example, in contrast to the CDR's focus on better consumer choice between commercial competitors, the development of the GDPR is seen to have moved from 'a market-oriented framework to one where fundamental rights are of central importance.'<sup>12</sup>

<sup>11</sup> Accenture, 'Tech Giants, Online retailers face uphill battle pursuing bank market share in Australia, but new 'Open Banking' Rules could tilt landscape, Accenture research finds' (25 July 2018) <<https://newsroom.accenture.com/news/tech-giants-online-retailers-face-uphill-battle-pursuing-bank-market-share-in-australia-but-new-open-banking-rules-could-tilt-the-landscape-accenture-research-finds.htm>>.

<sup>12</sup> EU General Data Protection Regulation, Recital 6; GDPR article 88.

The issue of consent has been a point of difficulty for businesses operating under the GDPR, with actions being taken against organisations for wrongly relying on consent to process personal data.<sup>13</sup> As consent must be unambiguous and cannot be inferred, it is important that clear guidance is provided under the law and regulations regarding what is acceptable consent. Currently, under Division 4.3 of *Competition and Consumer (Consumer Data Right) Rules 2020*, details are provided however they are unclear and refer to the Consumer Data Standard. To promote innovation and clarity for third party providers and the customers, the rules regarding consent should be made unequivocally clear.

The OAIC states that it is the businesses' responsibility to ensure that withdrawal of consent is as easy as giving consent, and 'must inform individuals about this right to withdraw consent'.<sup>14</sup> However, the ACCC's Digital Platforms Inquiry notably proposes that the definition of consent should be strengthened, recommending the introduction of notification and erasure rights for consumers' personal information.<sup>15</sup> The LIV considers this focus on consumer protection and empowerment to be better placed to realise the expansion of the CDR, rather than relying on regulation of market actors responsible for collection and storage of data. Given the complexities raised by information asymmetry and accessibility, strengthening consumer choice should be preferred.

### 3. *Adequate resourcing and funding to regulatory bodies*

The recent Royal Commission shed light on the banking industry, exhibiting a failure in regulatory oversight and in responsibility and accountability taken by the banking and financial services sector.

<sup>13</sup> C-507/17, Google LLC v. CNIL, 2019 EUR-Lex CELEX No. 62017CJ0507 (Sept. 24, 2019) <[http://curia.europa.eu/juris/document/document\\_print.jsf;jsessionid=FF2068A68B302A60C12B4191B752D64D?docid=218105&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=1704403](http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=FF2068A68B302A60C12B4191B752D64D?docid=218105&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=1704403)>, Claire Edwards, Limitations of consent shown in GDPR cases, (Web Page, 28 August 2019) <<https://www.pinsentmasons.com/out-law/news/limitations-of-consent-shown-in-gdpr-cases>>.

<sup>14</sup> EU General Data Protection Regulation, art 7(3); Office of the Australian Information Commissioner, 'Australian entities and the EU General Data Protection Regulation (GDPR) (8 June 2018) <<https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation/>>.

<sup>15</sup> Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Preliminary Report* (Report, 10 December 2018) <<https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/preliminary-report>>.

In order to successfully prohibit on-selling CDR data, aggregation of CDR data to build profiles of third parties, and the use of CDR as marketing tools for other products, sufficient scrutiny must be made mandatory across all sectors for which the CDR is developed, along with funding of the relevant agency tasked with such supervision.

While it has been noted that the funding of the ACCC and OAIC is a matter for the government, we do note the heavy burden to be placed upon the ACCC and OAIC and the excellent work already being undertaken by these organisations;<sup>16</sup> alongside their roles as watchdog and competition and consumer rights regulator. As such, we recommend regular review of ACCC and OAIC resourcing to ensure that these agencies are capable of completing their oversight responsibilities to the necessary standards. The LIV commends the additional funding provided to the OAIC following the ACCC's Digital Platforms Inquiry report.<sup>17</sup> However, at present we would argue that the policing role left to the OAIC as an adjunct to the Notifiable Data Breach scheme is absent adequate funding, staffing and support.<sup>18</sup> This needs to be addressed prior to any additional expectations (much less obligations) added to their present core responsibilities. Further, whilst the LIV is supportive of the dual role provided to the ACCC and the OAIC under the regime, the government should be mindful this is not a traditional area for the ACCC. As such, the government will need to monitor the delegation of matters between OAIC and ACCC, to ensure staffing at each organisation aligns with the technical requirements of the matters being referred. This could be a notable source of increasing the burden of work on the OAIC if their resources are not increased and the ACCC are not prepared to take on the more complex matters with existing staff.

<sup>16</sup> Office of the Australian Information Commissioner, 'Commissioner launches Federal Court action against Facebook' (Web Page, 9 March 2020) <<https://www.oaic.gov.au/updates/news-and-media/commissioner-launches-federal-court-action-against-facebook/>>.

<sup>17</sup> Natish Patel, Aayush Jaun, 'Government to enhance data privacy and protection to 'regulate the digital age'', Gilchrist Connell (Web Page, 20 January 2020) <<https://www.gclegal.com.au/lime-light-newsletters/government-to-enhance-data-privacy-and-protection-to-regulate-the-digital-age/>>.

<sup>18</sup> Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Preliminary Report*, (Report, 10 December 2018) 13-14 <<https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/preliminary-report>>.



Australia has seen a welcome increase in the notification of data breaches since the introduction of the Notifiable Data Breaches scheme. However, Australia's notification rate remains significantly lower than many European nations under the GDPR.<sup>19</sup> The OAIC's recent report on the types of data breaches notified under the scheme found that an overwhelming majority of breaches were a result of the 'malicious or criminal attacks,'<sup>20</sup> aimed at exploiting consumer data for financial gain. In line with Accenture's findings that two-thirds of Australian consumers are concerned with the management of financial data, the OAIC report found that 37 per cent of personal information involved in the breach included financial details, such as bank account or credit card numbers.<sup>21</sup> Successful expansion of the CDR into the banking sector would need to better safeguard consumer protection and engender consumer trust. The 'My Health Record' initiative, which saw 2.5 million Australians choose to opt out of allowing their patient data to be made available to health practitioners.<sup>22</sup> This suggests a need to address the general public's concerns about data mismanagement before its expansion. The aforementioned recommendation to introduce a right closely aligning with the GDPR's 'right to be forgotten',<sup>23</sup> would improve consumer trust and engagement more broadly with the idea of sharing data.

The ACCC has acknowledged that information asymmetry and power imbalances affect people's capacity to demonstrate consent and exercise choice.<sup>24</sup> Of particular concern are 'vulnerable consumers' – who are vulnerable for reasons such as disability, low education levels and financial pressures. Such consumers are at risk of not having capacity to fully understand what providing their

<sup>19</sup> DLA Piper, 'GDPR Data Breach Survey 2020' (Web Page, 20 January 2020) <<https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/>>.

<sup>20</sup> Office of the Australian Information Commissioner, 'Notifiable Data Breaches Report' (February 2020) 8.

<sup>21</sup> Ibid.

<sup>22</sup> Christopher Knaus 'More than 2.5 million people have opted out of My Health Record' (Web Page,, 20 February 2019) <<https://www.theguardian.com/australia-news/2019/feb/20/more-than-25-million-people-have-opted-out-of-my-health-record>>.

<sup>23</sup> EU General Data Protection Regulation, Article 17.

<sup>24</sup> Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Preliminary Report* (Report, 10 December 2018) 8 <<https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/preliminary-report>>.

consent means regarding data. While public education may go some way in mitigating this risk, there remains a general concern about a lack of engagement and apprehension amongst much of the public regarding how their data is being used. Both situations risk consumers merely scrolling and clicking through disclosures and consent agreements without understanding how their data will be used. These concerns have also been expressed in relation to the 'Online Banking' CDR regime, and it is likely that the risks will only increase with the expansion across sectors.

The LIV suggests a perspective that recognises knowledge and accessibility challenges to especially vulnerable people such as:

- Minors under the age of 18;
- Individuals whose language skills are insufficiently developed/foreign and lack proper capacity to consent/and or recall consent;
- Individuals who are mentally, physically, geographically or otherwise challenged;
- Individuals who are aged over 70 years old, where they have limited knowledge of and experience with technology;
- Individuals whose data has been given without their consent for example by a partner, spouse, parent, relative and who are not aware of the sharing let alone how to correct or delete such records held by other organisations.

#### 4. Opportunity to address and clarify inconsistencies in the legislative regime

The LIV queries whether CDR participants in 'Online Banking', the banks and other sectors with access to, and responsibility for, the data – will fully understand their rights and obligations under the complex regime. They will need to comply with multiple sets of privacy regulations, and regulations relating to their respective sectors. While strong penalties to deter non-compliance have been recommended, the complexity of the current regime risks unduly punishing participants who are trying to understand their responsibilities to consumers. Especially for SMEs in the sector, the legal and technical compliance cost could be substantial and potentially even prohibitive to the entry of new businesses into the sector.



Recent litigation on the topic has not sufficiently clarified the legislative definition of what constitutes ‘personal information’ for the purposes of data collection. In *Productivity Commissioner v Telstra Corporation Limited* [2017],<sup>25</sup> the appeal arose due to differences in the way in which the Privacy Commissioner and the AAT approached interpretations of ‘personal information’. With the Federal Court consideration limited to narrowly defined grounds of appeal, the court was only required to determine the meaning of the phrase ‘about an individual’, and only provided guidance in assessing whether information meets the definition ‘personal information’.

Further guidance is needed by the courts or through legislative amendment regarding ‘the precise meaning and scope’ to ensure organisations better understand when information collected becomes ‘personal information’. Guidance should reconcile Australia’s protection of ‘personal information’ with the GDPR’s broader protections of ‘any information relating to an identified or identifiable natural person<sup>26</sup>, which can include ‘inferred’ or ‘derived data’ created about individuals. Responding to the absence of clear guidance from the court, the Productivity Commission recommends the development of sector-specific standards for data sharing, ensuring that in absence of industry agreement, ‘consumer data’ should default to a broad definition.<sup>27</sup> Organisations collecting and storing data should adopt a precautionary approach, ensuring that where there is doubt, they should treat the information as ‘personal information’ for the purposes of protection and secure handling.

The interaction between the Australian Privacy Principles and the new CDR Privacy Safeguard Guidelines,<sup>28</sup> requires clarification as disjunction between privacy regimes can affect the choice to use, store and secure personal information and CDR data. Such complexity, particularly as the CDR regime is rolled out into other sectors beyond banking, could undermine the economic benefits hoped to be obtained through increasing the ability of organisations to share and utilise data. The LIV supports the Productivity Commission recommendation to enact entirely new legislation (*‘Data*

<sup>25</sup> *Productivity Commissioner v Telstra Corporation Limited* [2017] FCAFC 4.

<sup>26</sup> EU General Data Protection Regulation, art. 4.1.

<sup>27</sup> Productivity Commission, ‘Data Availability and Use’ (Inquiry Report No 82, 31 March 2017) 57.

<sup>28</sup> Office of the Australian Information Commissioner, ‘CDR Privacy Safeguard Guidelines’ (24 February 2020) <<https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/>>.

*Sharing and Release Act'*),<sup>29</sup> rather than amending the existing *Privacy Act 1988 (Cth)* or introducing a third general data protection regime that did not otherwise seek to replace or combine either the Privacy Act and the CDR regimes. The LIV believes the Productivity Commission recommendation will combat the confusion caused by the complexity and burden of satisfying two over-lapping privacy regimes.

*5. Introducing proportionate penalties for breach and misuse of data.*

In the United Kingdom ('UK') sitting alongside the GDPR is the Privacy and Electronic Communications (EC Directive) Regulations 2003, which provide for a private right of action to allow a private plaintiff to bring an action for compensation if they suffer damages from a violating of their data; beyond any contractual right.<sup>30</sup> Such a legislative instrument could be established specifically relating to the CDR, instead of relying on the Australian Consumer Law. This could assist in enforcing the goal of protecting consumers.

As a preventative measure to mitigate organisations seeking to overstep their collection and on-sale of data beyond what they need, the LIV recommends penalties for the misuse of data must include custodial, not just financial penalties. In the same way occupational health and safety offences can result in relevant office holders being imprisoned.<sup>31</sup> Custodial penalties are deterrents for companies who may otherwise be willing to absorb financial penalties if they are outweighed by the benefits of misusing the data. Such laws however, must be carefully tailored as to ensure they only address conduct within the control of the relevant officeholder charged. An alternative approach would be to emulate that UK's *Data Protection Act 2018*, which sets new standards for protecting personal data, in accordance with the GDPR and includes criminal offences. This legislation, rather than dealing solely with banking data and misuse under data obtained, takes a wholistic approach to personal data and its use rather than specifically the uses under the CDR. For example, section 170 criminalises knowingly or recklessly retaining personal data (which may have been lawfully obtained) without the consent of the data controller or criminalises knowingly or recklessly obtaining,

<sup>29</sup> Productivity Commission, 'Data Availability and Use' (Inquiry Report No 82, 31 March 2017) 308.

<sup>30</sup> Privacy and Electronic Communications (EC Directive) Regulations 2003 reg 30.

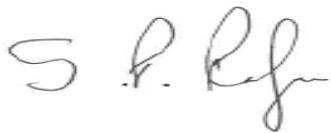
<sup>31</sup> Work Health and Safety Act 2011 (Cth) s31.

disclosing or procuring personal data without the consent of the data controller, and the sale or offering for sale of that data.

In summary, the LIV supports the availability of both financial and imprisonment penalties, regular reviews of activities to ensure compliance, and a period of closer supervision post-penalty akin to a term of 'bailment'.

Should you wish to discuss this further, please contact LIV Policy Lawyer Maurice Stuckey on (03) 9607 9382 or [mstuckey@liv.asn.au](mailto:mstuckey@liv.asn.au).

Sincerely



Sam Pandya

**President**