

more  
than  
money



# Lessons Learned from Australia and the United Kingdom

## The Consumer Data Right and Open Banking

Brad Carr, Alysia Abeyratne and Claire Melling



NatWest

# Executive Summary

Both the UK and Australia have enacted regimes which mandate the sharing by banks of customer data with third parties, with customer consent. Both regimes share similar policy underpinnings: to increase competition, innovation and empower consumers with control over their data. However, the two countries have diverged in their journeys to implementing these frameworks, notably in relation to their respective scope in terms of 'breadth versus depth.' The UK system was designed from the outset with depth of functionality in mind, whereas Australia has leaned towards breadth of data sharing across the economy.

Whilst Australia's Consumer Data Right ('CDR') regime was modelled on the United Kingdom's ground-breaking Open Banking framework, it departed from its predecessor, which confined itself to the sharing of banking information and to payment services. Australia's regime is now globally unique in its intended breadth of coverage as a whole of economy data portability framework. In this regard, many would argue, the CDR has been prescient in its ambition. Equally though, the depth of the functionality of the UK Open Banking regime (beyond mere read access), is often lauded as a having 'turbo-charged' the regime in terms of consumer uptake and the sophistication of product offerings.

The UK and the Australian regimes are now at a critical juncture of their respective development, with the UK looking beyond banking and finance to open data<sup>1</sup> and Australia shifting focus to 'system functionality and growth.'<sup>2</sup> Three to four years on, is Open Banking in the UK and the CDR in Australia heading in the right direction? And are they moving quickly enough to be impactful in their respective economies?

We contend that both countries are heading in the right direction, however, reform is needed to ensure that these regimes keep pace with technological change and achieve their potential to enable greater competition, innovation and ultimately deliver benefits to consumers in both nations:

1. Both jurisdictions should keep in mind global interoperability to ensure they remain at the forefront of technology-led trade and look beyond a sectoral approach and towards "Open Data."<sup>3</sup>
2. As Australia extends the CDR to action initiation and across sectors, Australia should learn from the UK's successes in building on existing legal frameworks and infrastructure, rather than duplicating regimes.
3. Australia should look to mirror aspects of the effective collaboration between industry and regulators in implementing the Open Banking regime, including considering a role for a purpose-built implementation entity that heeds the experience of the UK's OBIE.<sup>4</sup>
4. The UK should continue to take a forward leaning approach, as Australia has done, in extending Open Banking to be an economy wide data sharing regime.
5. Both countries should embed a role for digital identity, without which the regime will not be able to scale and deliver the promised benefits to consumers and the economy.<sup>5</sup>



1 Gavin Littlejohn, Ghela Boskovich, and Richard Prior, 'United Kingdom: The Butterfly Effect' in Jeng, Linda (ed), Open Banking (Oxford University Press 2022) 196.

2 Elizabeth Kelly PSM, Statutory Review of the Consumer Data Right (Report September 2022) 3.

3 Ron Kalifa OBE, 'Kalifa Review of UK Fintech' (Report February 2021), 26. The Kalifa Review recommended taking "a cross-sectoral approach to Smart Data.. [mandating]... the sharing of data not just within sectors (such as Open Banking), but also between sectors." It also referenced the EU's Data Strategy [which] recognises the need to look at "data spaces" across multiple industries.

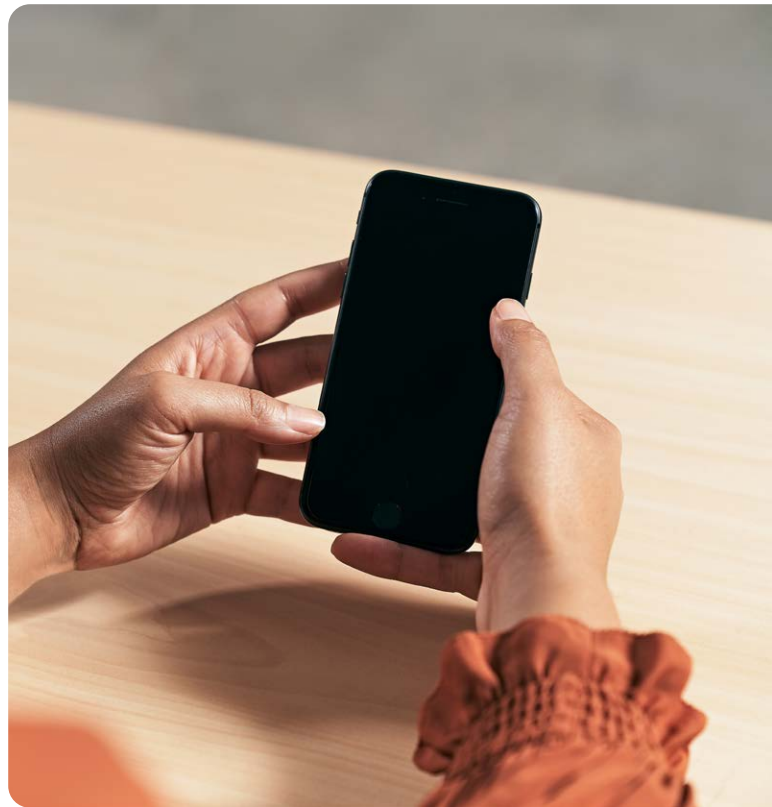
4 'Working group formed to determine the future of UK open banking' Finextra, 10 August 2022, <https://www.finextra.com/newsarticle/40783/working-group-formed-to-determine-the-future-of-uk-open-banking>. Whilst we note that in the UK the role of the OBIE is ending as the CMA Order is completed, a similar body 'with a more broadly-based funding and governance model' will be appointed as a successor. It is a commonly held view that the OBIE played a significant part in the UK's successful implementation of Open Banking.

5 'Sibos 2022: Open banking in the UK - it's high time for a review' Finextra, 11 October 2022, citing comments from Dan Globerson.

# Introduction

Open Banking has been in place in the UK since 2017<sup>6</sup> and the CDR was enacted in mid-2019 in Australia.<sup>7</sup> Briefly put, Open Banking is a mandatory framework which enables consumers and business to securely share their banking data with third parties and also enable third parties to make payments on their behalf. By contrast, the CDR is an economy wide data sharing regime, which is being rolled out on a sectoral basis. The first sector to be designated was banking. The CDR requires Authorised Deposit Taking Institutions (banks) to securely share certain product and customer information with accredited third parties with a customer's consent to provide goods or services. In the following sections, we will:

1. Consider the commonalities and differences in the policy underpinnings and the legislative approaches in each jurisdiction.
2. Analyse adoption, implementation rates and key use cases of Open Banking in the UK and CDR in Australia.
3. Identify lessons learned for both jurisdictions (in relation to governance, regulatory design, and implementation) and aspirations for the future of the CDR in Australia and Open Banking in the UK.



## 1. Common threads that bind – policy foundations of the regimes

Both the UK Open Banking regime and Australia's CDR framework arose out of similar policy settings, namely a view that increased data sharing would offer the potential for greater competition (particularly in concentrated markets), enable the development of alternative business models, and improve choice and customer outcomes.

Concentration in the banking sector in the UK was of significant concern to the Government, with the 2008 Global Financial Crisis said to have 'undoubtedly worsened the position.'<sup>8</sup> In the UK, the Fingleton Report, commissioned in 2014 by HM Treasury, explored this further and recommended, amongst other things, bank-led open Application Programming Interface (API) standards to enable data access and an industry-wide approach for authorising third parties to access banking data.<sup>9</sup> Similarly, Australia's CDR had origins in recommendations arising out of successive competition inquiries and Parliamentary inquiries into banking which identified the potential benefits of data sharing on competition and consumer choice, leading up to the Productivity Commission Inquiry into Data Availability and Use.<sup>10</sup> In 2017, the Government announced it would introduce an economy wide data sharing framework, with implementation to be prioritised in certain sectors, with banking being the first cab off the rank.<sup>11</sup> The mammoth task of designing the architecture of such an ecosystem was the purview of the Farrell Report which was an independent report commissioned by the former Government to advise on the best approach to implement Open Banking in Australia.<sup>12</sup>

<sup>6</sup> The legal mandate for the UK's largest nine banks (CMA9) to provide authorised entities with access to customer banking data via secure API was enacted through the CMA's Retail Banking Market Investigation Order 2017.

<sup>7</sup> The Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth) received Royal Assent on 12 August 2019 and commenced on 13 August 2019.

<sup>8</sup> See Fingleton J, Speech at the seminar on 'A competitive banking sector: Challenges in a post-crisis environment' organised by MLex in association with Lloyds Banking Group, <https://fingleton.com/wp-content/uploads/2014/10/Competition-in-UK-banking-16-Feb-2012.pdf>.

<sup>9</sup> Open Data Institute and Fingleton Associates 2014, Data Sharing and Open Data for Banks: A report for HM Treasury and Cabinet Office. [http://www.fingletonassociates.com/wp-content/uploads/2014/12/141202\\_API\\_Report\\_FINAL.pdf](http://www.fingletonassociates.com/wp-content/uploads/2014/12/141202_API_Report_FINAL.pdf). Around the same time, the UK CMA also conducted a Market Inquiry into the supply of personal current accounts and retail banking services to SMEs, with its final report issued in 2016, with similar findings about the need for increased competition and data sharing. See: CMA, 'Retail Banking Market Investigation: Final Report' (9 August 2016) [http://www.fingletonassociates.com/wp-content/uploads/2014/12/141202\\_API\\_Report\\_FINAL.pdf](http://www.fingletonassociates.com/wp-content/uploads/2014/12/141202_API_Report_FINAL.pdf)

<sup>10</sup> Note in particular Scott Farrell 'Review into Open Banking: Giving Customers choice, convenience and confidence' (Report December 2017), 2; 2014 Financial System Inquiry (the 'Murray Inquiry'); 2015 Competition Policy Review (the 'Harper Review'); 2016 the Report of the House of Representatives Standing Committee on Economics' Review of the Four Major Banks (the 'Coleman Report').

<sup>11</sup> Australian Government, "Open Banking: Customers, Choice, Convenience, Confidence" ("The Farrell Report") (Dec. 2017). <https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-For-web-1.pdf>, page 3.

<sup>12</sup> See Hon Scott Morrison MP, (9 May 2017), 'Building an accountable and competitive banking system', <https://ministers.treasury.gov.au/ministers/scott-morrison-2015/media-releases/building-accountable-and-competitive-banking-system>



# Differences in approach – breadth vs depth

## Australia's CDR: broad scope and new legal frameworks

The Farrell Report found that there was no “compelling reason why the banking sector could not be regulated by a framework that can also apply to other industries,”<sup>13</sup> provided the risks of each sector were specifically considered and accommodated within the ecosystem.<sup>14</sup> With the breadth of the Government mandate in effect, Australia set upon a bold path of creating a legislative framework to mandate economy wide data sharing.

Two years on and following rounds of stakeholder consultation, the CDR regime was enacted through legislation,<sup>15</sup> a sectoral designation instrument<sup>16</sup> and CDR Rules.<sup>17</sup> The regime also includes Data Standards regarding the format and process for data transfer and Consumer Experience Guidelines which set out both best practice and also certain minimum experience guidelines with which participants in the CDR ecosystem need to comply. Many would agree that the codification of the CDR across these different legislative instruments has resulted in a high level of complexity and compliance overhead for participants.<sup>18</sup>

## UK Opening Banking: existing legal frameworks and depth of functionality

Contrastingly, the UK's Open Banking regime was largely legislated through the EU's General Data Protection Regulation ('GDPR') and the revised Payment Services Directive ('PSD2'), which was embedded into law by the Payment Services Regulations (2017) UK. Unlike Australia, however, the UK already had an extremely robust privacy regime, with a strong consent framework in the form of the GDPR.<sup>19</sup> PSD2 also played an important part in the design of Open Banking, as it required the UK to adopt the EU framework by January 2018.<sup>20</sup>

*To this end, 'depth' in the functionality of Open Banking beyond mere data sharing was inbuilt as part of its initial scope.*

Building on this framework, the Competition and Markets Authority ('CMA') ordered the UK's nine largest banks (the 'CMA9') to meet the requirements of PSD2 in a standardised way.<sup>21</sup> As the CMA Order was outcome driven, the implementation plan has required the CMA9 to deliver more functionality than PSD2 (for e.g., refunds and variable recurring payments functionality). The CMA's Order also established the Open Banking Implementation Entity ('OBIE'), which was governed and funded by the CMA9 and was tasked with overseeing the roll out Open Banking, including determining API specifications, managing the accreditation registry, monitoring CMA9 conformance with standards, providing guidance and managing disputes and complaints.

While the UK's Open Banking regime is not without its own complexity, it does appear to have taken on a more incremental approach, building on an existing robust privacy framework in the GDPR and avoiding regulatory duplication in this regard. This could be contrasted with the regulatory position in Australia, where arguably Australia has created two distinct and sometimes overlapping data protection regimes, which may govern the same kind of data differently depending on source (i.e., whether data, which could also be considered 'personal information' is obtained through the CDR Rules or obtained outside of the CDR ecosystem, where the Privacy Act 1988 (Cth) applies). This creates a level of inconsistency in the Australian framework which presents challenges for implementation of the regime.

---

<sup>13</sup> Scott Farrell 'Review into Open Banking: Giving Customers choice, convenience and confidence' (Report December 2017) 3.

<sup>14</sup> Ibid.

<sup>15</sup> The Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth) established in Pt IVD of the Competition and Consumer Act 2010 (Cth) ("CCA") the general framework for the CDR, including privacy safeguards that would apply to 'CDR data,' roles of relevant regulators, and powers for the Minister to designate sectors of the economy to which the CDR would apply.

<sup>16</sup> Banking was the first sector to be designated per the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 (Cth). The Energy and Telecommunications sectors followed: Consumer Data Right (Energy Sector) Designation 2020 (Cth); Consumer Data Right (Telecommunications Sector) Designation 2019 (Cth).

<sup>17</sup> The legislation was complemented by the Competition and Consumer (Consumer Data Right) Rules 2020 ("CDR Rules"), which established the mechanics of the regime, including a uniquely prescriptive consent framework, prohibitions on use of CDR data, dispute resolution and accreditation models and processes.

<sup>18</sup> Elizabeth Kelly PSM, Statutory Review of the Consumer Data Right (Report September 2022) 46.

<sup>19</sup> The GDPR was required to be implemented by all EU member states by 25 May 2018. The UK enacted the GDPR through the Data Protection Act 2018 (UK).

<sup>20</sup> PSD2 was legislated through changes to the Payment Services Regulation (2017) (UK), which also mandated strong customer authentication in line with PSD2. See in particular Pt 7 of the Payment Services Regulation (2017) (UK).

<sup>21</sup> The legal mandate for the UK's largest nine banks (CMA9) to provide authorised entities with access to customer banking data via secure API was enacted through the CMA's Retail Banking Market Investigation Order 2017.



# 2. Adoption, implementation, and key use cases

## The UK experience – deeper functionality driving adoption

A key feature of Open Banking in the UK is the ability for a consumer to do more than direct the sharing of their data (sometimes termed ‘action initiation’ or ‘write access’), and this will be a key driver in the ultimate success of Australian’s CDR regime. This is already playing out in other jurisdictions, noting that globally “a third of fintech built with open banking and open finance are payment solutions.”<sup>22</sup> Certainly, the increasing rate of adoption of Open Banking in Europe could be viewed as an indicator of Buckley and Jevglevskaia’s proposition that action initiation is “petrol in the engine”<sup>23</sup> for Open Banking as it has been projected that in the coming years, Open Banking users in Europe are “expected to increase to 68.3 million by 2024, up from 12.2 million in 2020.”<sup>24</sup> Payments and lending are the most popular use cases, with financial management tools trailing behind.<sup>25</sup> This supports the view that consumers are wanting deeper functionality and the ability to direct their data for particular uses, rather than simple analytic insights delivered by these kinds of PFM tools.

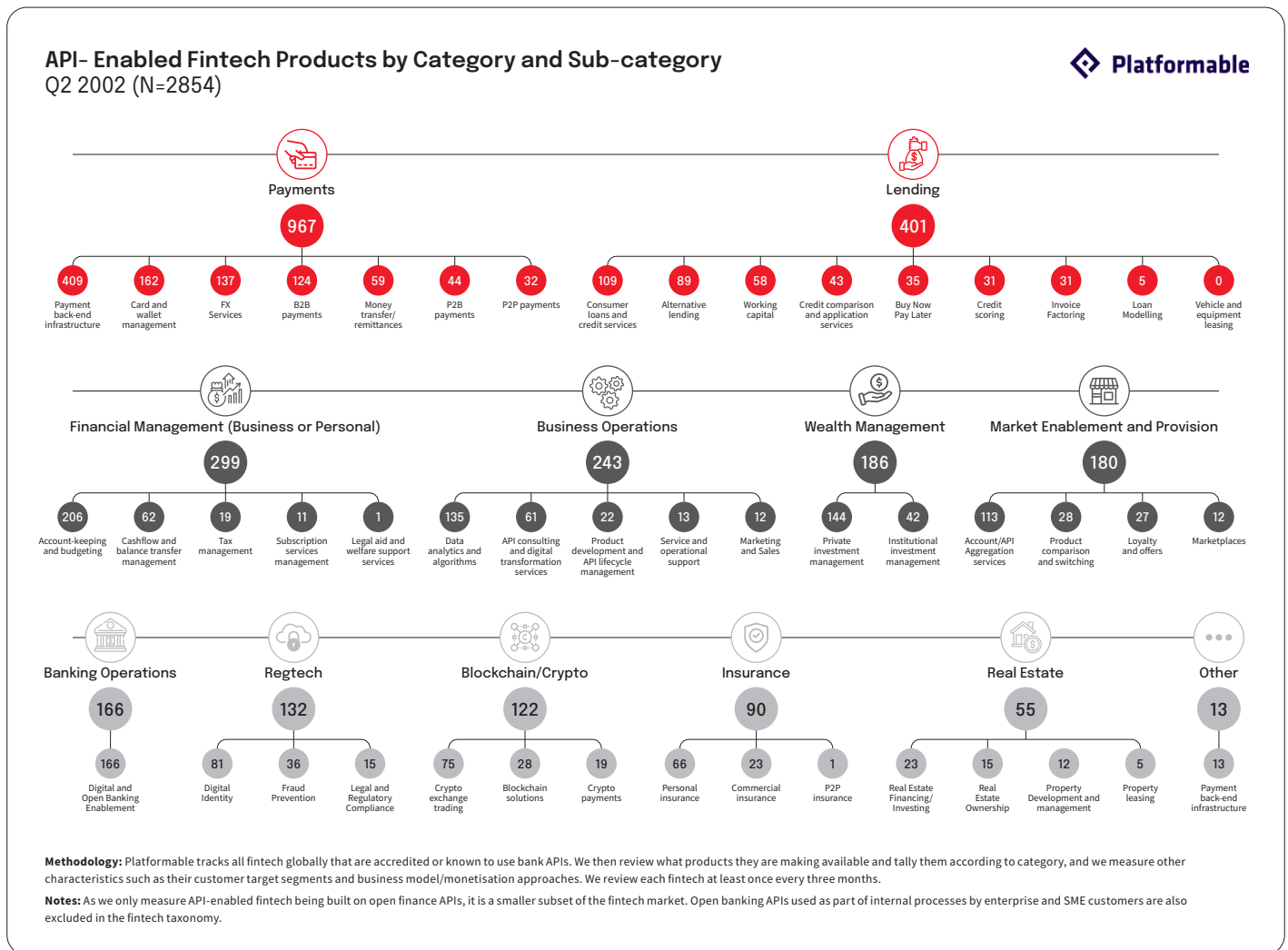


Figure 1- Adapted from Platformable API-Enabled Fintech Products by Category and Sub-Category<sup>26</sup>

22 Pham, Perkins and Boyd - Platformable: “Open Banking/Open Finance Trends Q3 2022, Data and Trends Overview, July 2022” 24.

23 Scientia Professor Ross Buckley and Dr Natalia Jevglevskaia, Submission to the Statutory Review of the Consumer Data Right (September 2022) 3.

24 Pham, Perkins and Boyd - Platformable: “Open Banking/Open Finance Trends Q3 2022, Data and Trends Overview, July 2022” 26.

25 See Figure 1 below.

26 Pham, Perkins and Boyd - Platformable: “Open Banking/Open Finance Trends Q3 2022, Data and Trends Overview, July 2022”, 24.

According to the OBIE “in March 2022, the number of payments reached 4.5m and the month-on-month growth rate is running at 10%.”<sup>27</sup> There are approximately 6.5 million customers that currently use Open Banking, which equates to 10% of the UK’s adult population. In October 2022 there was over 1 billion successful API calls with CMA9 banks.<sup>28</sup> There are currently 70+ banks and 249 Third Party Providers (TPPs) in the ecosystem.

Open Banking is also delivering tangible value to small business in the UK through integration with cloud accounting platforms. Recently, the OBIE referenced that 77% of SMEs surveyed reported having more immediate and accurate insights into their financial position by using these services, and 84% reported that cloud accounting led to them feeling more efficient.<sup>29</sup> Data sharing of this kind has the potential to be transformative for businesses in enhancing productivity by automating low value, high resource intensive financial management activities, and obtaining more accurate and real time insights regarding cashflow and business performance.

In Australia, where the CDR is still relatively nascent, uptake has been fairly slow. There are 76 data holders and 32 accredited data recipients on the register, 20 of which have an ‘active’ status. Though, according to Frollo, in the first year of Open Banking, the Frollo money management app “was responsible for more than 95% of all Data Recipient API calls in Australia.”<sup>30</sup> Presently, the CDR offerings in Australia relate to account aggregation, personal financial management tools and CDR powered credit applications. That said, from November 2022, customer data sharing commenced for the major energy providers and the AEMO and in January this year the Telecommunications sector was designated. Australia is therefore likely to start seeing cross-sectoral innovation opportunities such as financial institutions ingesting energy data to provide customers with insights and ‘green financing’ offers for solar or batteries. Consumers will see benefits as they are able to consent to the sharing of their banking and energy data, which could help manage cost of living pressures, through tracking energy usage and estimating future bills.



27 OBIE ‘Open Banking Impact Report June 2022 – key insights on adoption and business use’ <<https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-june-2022/>>

28 See API Performance Statistics available at <<https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-june-2022/>> accessed December 2022.

29 OBIE ‘Open Banking Impact Report June 2022 – key insights on adoption and business use’ <<https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-june-2022/>>

30 Frollo State of Open Banking (Report 2021) 10. <<https://frollo.com.au/open-banking/the-state-of-open-banking-2021/>>.

# 3. Lessons learned and aspirations for the future of the CDR in Australia and Open Banking in the UK

## A role for an implementation agency to oversee the roll out of the CDR in Australia?

As a ‘second mover,’ Australia has the opportunity to learn from the UK Open Banking Experience. One such lesson is the immense benefit associated with strong industry and government collaboration, where each have an important role to play. This was borne out in the UK through the partnership between the CMA and OBIE in overseeing and delivering the technical standards for Open Banking. As Littlejohn, Boskovich and Prior describe:<sup>31</sup>

*“While the CMA had put a lot of effort into the design of the governance and funding model, they did very little in commenting on technical design choices, other than to require that they be standardized and align with PSD2. The outcomes-based approach of the Order was of critical importance in the years ahead... This approach, rather than a highly prescriptive order, has been one of the most important contributions to the success of Open Banking in the United Kingdom.”*

The CDR regime is a challenging, multi-party technology project. Indeed, as the ACCC aptly noted in its submission to the Statutory Review of the CDR, with regard to its role as the Accreditation Registrar:<sup>32</sup>

*The build, continued development, maintenance and operation of the Register is a complex and technical role... The ACCC has successfully built and continues to deliver a well-functioning register. This role has required the ACCC to substantially increase the skill set of its staff and has required adjustments to the ACCC’s governance framework... As the CDR program continues to expand, consideration should be given to whether this responsibility, skill set and capability are best aligned with the ACCC as regulator, or some other organisation.*

Similarly, the ACCC’s submission is also cognisant of the challenges associated with the ‘complexity’ and ‘velocity’ of the developments in the CDR ecosystem as new sectors are designated<sup>33</sup> and also notes as follows:<sup>34</sup>

*As the system continues to evolve, consideration should be given to arrangements that ensure that operational and implementation decisions are more clearly coordinated. Consideration should be given to consolidation or reallocation of some of the CDR’s roles and functions. The ACCC is supportive of a specialist agency being tasked with the implementation of the CDR. Further, the ACCC is supportive of a functional separation of the entities responsible for the rule-making, operations and enforcement. This mirrors the regulatory principles in many other mature markets, such as energy, and the UK’s open banking regulatory framework.*

This openness and invitation on the part of the ACCC presents an opportunity for the private sector in Australia to play a role and come to the table with suggestions on how to collaborate. As such, whilst we recognise the challenges (including funding) and the differences presented by an economy wide data sharing regime versus that of the UK with a banking focus, there could be some benefit in considering a role for a purpose-built implementation entity in Australia, that heeds the experiences of the UK’s OBIE (with the need for broader membership than banking and a strategic focus, looking across the economy irrespective of sectors). The UK experiences demonstrates that there is benefit, in certain areas of the system to industry led working groups, whose skills and expertise could be leveraged, with oversight by regulatory bodies. In particular, this is likely to be vitally important as Government looks to deepen the functionality of the CDR regime in Australia, with the establishment of action initiation, whilst at the same time that the scope of the regime expands to other sectors. In confronting technical issues such as interoperability with other rails (such as payments), the need for strong authentication measures and mitigating the myriad of other privacy, cyber and fraud risks associated with these changes, government should continue to utilise industry experience in capability in these areas. Ultimately, this is likely to provide benefits in terms of efficiencies and deliver value to consumers, participants, and the ecosystem as a whole.

---

31 Gavin Littlejohn, Ghela Boskovich, and Richard Prior, ‘United Kingdom: The Butterfly Effect’ in Jeng, Linda (ed), Open Banking (Oxford University Press 2022) 191.

Gavin Littlejohn, Ghela Boskovich and Richard Prior, United Kingdom: The Butterfly Effect In: Open Banking. Edited by: Linda Jeng, Oxford University Press 2022, pg.191

32 Australian Competition and Consumer Commission Submission (ACCC) Submission to the Statutory Review of the Consumer Data Right (September 2022) 4.

33 Ibid, 5.

34 Ibid, 7.

## UK to look beyond Open Banking

Where Australia can draw learnings from the UK's successful industry-government partnership and the role of the OBIE, commentators equally suggest that the UK can take lessons from the Australian experience. For example, it is often contended that the UK should have started with a whole of market approach to mandatory data sharing, as Australia has done. As Buckley, Jevglevskaia and Farrell note, "in contrast to Europe, Australia's approach is more sensitive to the practical reality of how data operates in the real world, as it does not discriminate between the origins of data."<sup>35</sup>

Certainly, it appears that the UK Government is live to this issue as the Smart Data Working Group has recommended building on Open Banking to expand to other regulated sectors (such as finance, telecommunications, energy and pensions) as part of its Smart Data Initiatives.<sup>36</sup>

In building out the regime to these sectors, the Australian experience would caution against duplication and inconsistency in privacy and data security frameworks, which can lead to disincentives for players to join the ecosystem, particularly if regulatory costs and compliance burdens outweigh the perceived benefits of participation.<sup>37</sup> To the extent that existing privacy and security protections under the GDPR are adequate, these should be leveraged rather than creating a bespoke privacy regime for 'open data'. Similarly, there is likely to be benefit for the UK to adopting a principles-based regulatory approach, over prescription which means that rules are more easily adapted across sectoral boundaries<sup>38</sup> and allow for creative solutions in delivering compliant products and services.



# Aspirations for the future

## A new paradigm for competition – Open data

Today's environment brings with it a paradigm shift beyond the traditional approach to competition and the view of firms operating in strict verticals. The Report on the Statutory Review of the Consumer Data Right echoes this sentiment:<sup>39</sup>

*As Australia and the rest of the world move towards a more horizontally integrated economy, where businesses provide products and services that span traditional sector boundaries, the vertical structures between sectors will become increasingly blurred and consumers will expect a greater level of integration across different domains of their lives. The CDR is optimally placed to facilitate this and is on the precipice of doing so by providing a conduit from which businesses can compete across multiple sectors.*

With these notions in mind, Australia needs to build on its bold ambition for the CDR and look further than the sectoral approach to designation to ensure that the regime is still meeting its laudable aims for competition and consumer choice.<sup>40</sup> The same could be said of the UK, as its Smart Data initiative takes flight. To keep pace with the realities of business models, both nations need to truly take an economy wide approach to mandatory data sharing regimes. Otherwise, there remains a real risk in the future of entrenching market concentrations, particularly in the hands of firms that process the largest troves of data.

The need to move beyond sectoral constructs is vital, as this is where the greatest economic opportunities are likely to be found. Sectoral designation has been a key feature of the CDR and a similar structure is being adopted in the UK. In many respects this makes sense from an implementation standpoint. Ultimately, this approach may not create the conditions necessary (at the rate that is necessary) for innovation to thrive and for consumers to derive the most value from their data. If consumers are able to consolidate their data from different service providers across sectors to gain deeper insights, this would likely be more transformative, particularly in relation to firms with a large customer base where benefits could be provided to a broader group of individuals.

<sup>35</sup> Scientia Professor Ross Buckley, Dr Natalia Jevglevskaia and Scott Farrell Australia's Data Sharing Regime: Six Lessons for the World (2021) UNSWLRS 67 (Forthcoming in King's Law Journal), 33.

<sup>36</sup> See UK Smart Data Working Group Spring 2021 Report, 11. Under the draft legislation, Smart Data powers include: requirements on data holders to share, accept 'actions' and pay levies; requirements on TPPs to be authorised and pay charges; and responsibilities to sector regulators and other bodies to set standards, authorise participants, monitoring, complaints and enforcement.

<sup>37</sup> Elizabeth Kelly PSM, Statutory Review of the Consumer Data Right (Report September 2022) 46; 55.

<sup>38</sup> Ibid, 58.

<sup>39</sup> Ibid, 57.

<sup>40</sup> Brad Carr, 'From Open Banking to Open Data and Beyond: Competition and the Future of Banking' in Jeng, Linda (ed), Open Banking (Oxford University Press 2022) 303.



## A role for Digital Identity and Global interoperability

Finally, as both countries embark on cross sectoral implementation of the CDR and towards action initiation, it will be of vital importance to have an economy-wide mechanism to identify and authenticate individuals and businesses reliably and safely across the digital ecosystem. Any digital identity solution utilised for this purpose should be interoperable, provide strong privacy protections; ensure consumer empowerment and choice of authentication party; and integrate in a manner that provides a seamless customer experience. As we have previously noted,<sup>41</sup> both government and the private sector have a role to play in delivering this solution and collaboration between industry and the public sector will ensure alignment, leverage relevant expertise and avoid duplication of infrastructure.

## Seizing the opportunity: Digital Identity

In light of recent cyber incidents in Australia, we have seen an increased urgency to find a solution to minimise the amount of data required to be collected and held by organisations for identity verification purposes. Digital Identity can provide a solution as it may allow individuals to verify their identity (or an attribute, such as age), without the need for an organisation to collect personal information, or sensitive identity documents. In Australia, the Government commenced developing a framework for Digital Identity (the Trusted Digital Identity Framework, 'TDIF') in 2015 and consultation on Phase 3 of the Trusted Digital Identity Bill took place late 2021. Amongst other things, the legislation was intended to allow government and private sector bodies to participate in the Australian Government digital identity system.

Given the renewed focus on Digital Identity, it is an opportune time to revisit how it may interact with and complement the CDR. One of the recommendations of the Final Report into the Future Directions for the CDR (which was supported by Government) was that the CDR should 'continue to be developed in a manner that encourages the use of interoperable authentication solutions, based on compatible international standards.'<sup>42</sup> Under the current CDR regime, verification of a consumer's identity is not mandated (though there are Data Standards for authentication, which presently utilise a 'One Time Password'.)<sup>43</sup> It is clear, however, that as Australia's CDR regime deepens functionality to action initiation and as there is increased cross-sectoral data sharing, there will be a need to reliably verify a consumer's identity to safely enable these actions and data sharing.

For a Digital Identity system to be successful it will need to be trusted and secure and privacy must be inbuilt into the system design. Akin to the CDR and Open Banking frameworks, it should be consumer centric, with individuals having agency to choose which organisations verify their identity and for what purposes. Interoperability with CDR (and international standards and frameworks) will help generate broader take up and avoid fragmentation, which will ultimately lead to silos and no one system being effective.

A vision for what could be created was succinctly described in the Final Report into the Future Directions for the CDR as follows:

*When digital identity services are broadly adopted, the Inquiry envisages a future where consumers may be able choose from a market that includes government and commercial identity assurance providers, supporting consumers' choice of identity provider and allowing consumers to use the provider (or providers) they most trust with their personal information.<sup>44</sup>*

The time appears to be now to make good on this vision and Government and private sector developments<sup>45</sup> suggest that parties are convening around a shared goal.



41 Brad Carr "Digital Identity - Public and Private Sector Opportunities" <https://medium.com/@nabtechblog/digital-identity-public-and-private-sector-opportunities-384086088bbb>.

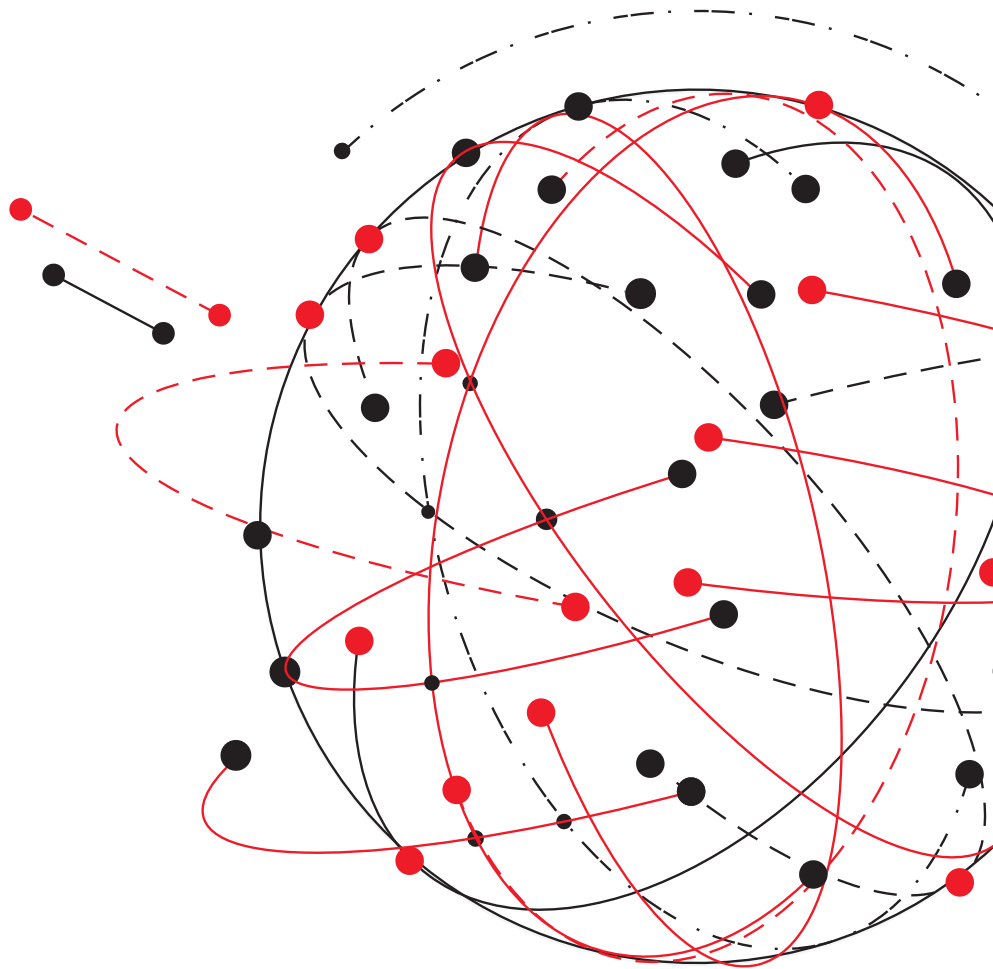
42 Scott Farrell 'Inquiry into Future Directions for the Consumer Data Right (Final Report, 2020), 184 (See in particular Recommendation 8.1.).

43 The Data Standards Board is currently reviewing the CDR authentication framework and alternatives to the use of 'One Time Passwords' for authentication.

44 Scott Farrell 'Inquiry into Future Directions for the Consumer Data Right (Final Report, 2020), 184.

This vision for the future could equally apply to the UK, where to date there has been limited success in rolling out a digital identity framework, with the UK's 'Verify' digital identity program slated to be retried in 2023, partly due to lack of take up, and cost overruns.<sup>46</sup>

Whilst 'Gov.uk Verify' will be phased out, a number of learnings appear to have been made from this experience. The UK Government consulted on a Digital Identity and Trust framework in 2021 (expounding similar principles to TDIF in Australia) and with a stated goal of global interoperability<sup>47</sup> and policy makers have also issued a clear direction that Digital Identity will be critical piece of the puzzle for the success of the UK's digital economy.<sup>48</sup>



45 See Department of Finance 'Data and Digital Ministers Meeting Communique' (4 November 2022) in particular section on 'Digital Identity' <<https://www.finance.gov.au/sites/default/files/2022-11/data-and-digital-ministers-meeting-communique-41122.pdf>> See also 'NAB backs ConnectID to help customers secure their identity' (31 August 2022) <<https://news.nab.com.au/news/nab-backs-connectid-to-help-customers-secure-their-identity>>.

46 See 'Parliamentary Secretary for the Cabinet Office, Julia Lopez MP 'Speech to The Investing and Savings Alliance', 18 March 2021 <<https://www.gov.uk/government/speeches/julia-lopez-speech-to-the-investing-and-savings-alliance>>

47 See [The UK digital identity and attributes trust framework - GOV.UK \(www.gov.uk\)](https://www.gov.uk)

48 Ron Kalifa OBE, 'Kalifa Review of UK Fintech' (Report February 2021), 9, 18. The UK Government has recently introduced legislation regarding digital identity and smart data, which may be passed in the second half of 2023.