1. Title: Australia’s Consumer Data Right and the Uncertain Role of Information Privacy Law

2. Article Category: Original Article

3. Summary:

- Data portability rights are viewed by policymakers worldwide as a significant legal innovation to stimulate competitive digital economies. These rights allow consumers and businesses to seamlessly receive and transfer data for commercialisation and efficiency purposes.

- The newly implemented Australian Consumer Data Right (CDR) provides an illuminating example of the complex relationship between information privacy and competition law which is central to data portability initiatives. The CDR grants consumers and businesses access and transfer rights for consumer data in the Australian banking, energy and telecommunications sectors, through the implementation of mandated API standards.

- There are three policy vectors at the heart of the CDR that parallel previous Australian, UK and EU data portability developments. They are the type of regulated data covered by the CDR scheme, privacy and security protections and the overarching regulatory framework.

- We argue that the CDR, and its antecedents, primarily construct data portability as a competition law measure. However, while the general policy intention of the CDR is clear, we contend that the scheme reveals an uncertain role for information privacy law as part of its operation. Uncertainty is evident in how policymakers have considered the information privacy law issues inherent in the three policy vectors.

- We contend that the CDR could give rise to definitional problems with regulated data, duplicated privacy and security protections and a conceptually challenging regulatory framework. In conclusion, we suggest potential solutions that would assist with the operation of the CDR within Australia’s broader information privacy law framework, governed by the Privacy Act 1988 (Cth), which would also better align with the General Data Protection Regulation (GDPR).

4. Keywords: Australian Privacy Principles (APPs), consumer protection, data portability rights, data protection, General Data Protection Regulation, principles-based regulation.
I. INTRODUCTION

“Having examined this approach, the Review considers that the amendments that would be required to the Privacy Act to implement the breadth of the CDR would not be minor… Perhaps most importantly, it has no clear competition-enhancing objectives.”

The above quote from the Open Banking Review (OBR) exemplifies one of the core challenges behind the newly implemented Australian Consumer Data Right (CDR). The CDR grants consumers and businesses access and transfer rights for consumer data in the banking, energy and telecommunications sectors, through the implementation of mandated API standards. However, successful implementation of the CDR, as with most data portability schemes, has been dependent on a careful consideration of information privacy law and competition law policy imperatives. It requires consideration of the costs and benefits of different possible conceptual bases, including portability of personal data based on information privacy purposes, and portability of consumer data based on competition law objectives. Successful data portability schemes also require consideration of the information privacy and security protections that will secure data transferred within either type of scheme. These issues are challenging in any jurisdiction but especially so in Australia with its weak information privacy law framework, as embodied by the governing Federal law, the Privacy Act 1988 (Cth) (Privacy Act).

Not surprisingly, therefore, the role of information privacy law in the operation of the CDR has been a prime point of policymaker contention. For example, The Productivity Commission envisioned a broad conceptual vision of a data portability scheme that utilised Australia’s existing information privacy framework for privacy protections, but noted

---

1 Review into Open Banking (Final Report, December 2017) 16 (‘Open Banking Review’).
2 Several Australian government inquiries have been conducted that are relevant to data portability, including information privacy law considerations. See Financial System Inquiry (Final Report, November 2014) (‘Murray Inquiry’); Competition Policy Review (Final Report, March 2015) (‘Harper Review’); Productivity Commission, Data Availability and Use (Final Report, Inquiry No. 82, May 2017) (‘Productivity Commission’); Review into Open Banking (Final Report, December 2017) (‘Open Banking Review’); Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Exposure Draft) (‘Consumer Data Right’). It should also be noted that for the purposes of this paper, information privacy law is used synonymously with data protection to reflect the Australian context.

2 Treasury Laws Amendment (Consumer Data Right) Bill 2018.
potential issues that need strengthening\textsuperscript{3}. Then, as a follow up to the Commission, the OBR placed greater critical emphasis on implementation issues by specifically examining whether and how the \textit{Privacy Act} could provide safeguards for a portability scheme.\textsuperscript{4} The OBR highlighted specific concerns but believed that the \textit{Privacy Act} should be amended to support the implementation of a new scheme. Finally, an entirely new approach was proposed by Treasury which obviated the \textit{Privacy Act}, in favour of a newly created, standalone set of CDR Privacy Safeguards housed in the \textit{Competition and Consumer Act 2010} (Cth), and whose substantive requirements are prescribed in sector-specific CDR Rules and Standards.\textsuperscript{5}

These different considerations outline the developmental tensions behind the CDR that are representative of broader policy conflicts involving data portability. As we demonstrate in this paper, the CDR has a clear policy priority predicated on the perspective of data portability as a competition law mechanism. However, we argue that the CDR has an uncertain role about information privacy law regarding its operation, especially in comparison to similar UK and EU developments. The uncertain role is evident across three policy vectors pertaining to the scope of regulated data in the CDR scheme: type of regulated data; privacy and security protections and regulatory framework.

Section II outlines the regulatory intersection of information privacy law and competition law in data portability schemes. The intersection is complex because it involves a combination of potentially conflicting policy priorities pertinent to the development of data portability. Section III compares the CDR against its policy predecessors and similar UK and EU developments, across the three policy vectors, highlighted above. Section IV demonstrates the uncertain role of information privacy law in the operation of the CDR by highlighting definitional problems involving CDR data and personal information under the \textit{Privacy Act}, the significant potential for duplication of information privacy obligations and the conceptually different foundations of the overarching regulatory framework. In conclusion, we argue that the CDR’s approach to information privacy could further weaken the application of Australia’s broader information privacy law framework and suggest that

\textsuperscript{3} Productivity Commission, \textit{Data Availability and Use} (Final Report, Inquiry No. 82, May 2017) (‘Productivity Commission’).

\textsuperscript{4} \textit{Review into Open Banking} (Final Report, December 2017) (‘Open Banking Review’).

\textsuperscript{5} Treasury Laws Amendment (Consumer Data Right) Bill 2019.
a closer alignment with the General Data Protection Regulation (GDPR) would be appropriate.

II. DATA PORTABILITY PERSPECTIVES

In keeping with other authors, we contend that there is an inherent information privacy subtext to data portability pertaining to individual control of personal information.6 However, unlike traditional information privacy mechanisms, data portability processes specifically focus on enhancing access and transfer capabilities for individuals.7

Initial policy perspectives considered data portability as a broad protector of personhood8 that regarded the formulation, recognition and protection of a fully flourishing digital personality, akin to its human form.9 Personality development, in this sense, was relevant across two axes.10 First, data portability mitigated against the entrapment of digital personhood. Portability aimed to prevent consumer service ‘lock-in’ by allowing individuals to transfer historical data from one service provider, to another, as a demonstrable verifier of trust.11 Second, data portability mechanisms acknowledged that an individual should be able to reap the full reward of their accumulated data history across different service providers.12 In other words, the human personality cannot develop fully without the freedom of

---

6 G Zanfir, ‘The Right to Data Portability in the Context of the EU Data Protection Reform’, (2012) 2 (3) International Data Privacy Law 149, 152; O Lysnkey, ‘Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability’, (2017) 42 (6) European Law Review 793, 811; L Edwards and M Veale, ‘Slave to the Algorithm? Why a ‘Right to An Explanation’ is Probably not the Remedy You Are Looking For’, (2017) 16 Duke Law and Technology Review 18, 72.
7 H Uršic, ‘Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control’, (2018) 15 (1) SCRIPTed: A Journal of Law 42, 47; Zanfir (n 6) 151; L Urquhart, S Neelima and D McAuley, ‘Realising the Right to Data Portability for the Domestic Internet of Things’ (2018) 22 (2) Personal and Ubiquitous Computing 317, 318.
8 Zanfir (n 6). See Bloustien, Edward J, ‘Privacy is dear at any price: A response to Professor Posner’s economic theory’, (1978) 12(3) Georgia Law Review 429 regarding the protection of personhood in a privacy context.
9 Zanfir (n 6) 151.
10 Both axes involve the type of individual empowerment envisaged by P De Hert and others, ‘The right to data portability in the GDPR: Towards user-centric interoperability of digital services’, (2018) 34 (2) Computer Law & Security Review 193, 200.
11 M Bilal Ünver, ‘Turning the Crossroad for a Connected World: Reshaping the European Prospect for the Internet of Things’, (2018) 26 (2) International Journal of Law and Information Technology 93, 2; Lynskey (n 6) 804.
12 Zanfir (n 6) 151; I Graef, ‘Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union’, (2015) 39 (6) Telecommunications Policy 502, 503; De Hert and others (n Error! Bookmark not defined.) 200; G Colangelo and M Maggiolino, ‘Data accumulation and the privacy–antitrust interface: insights from the Facebook case’, (2018) 8 (3) International Data Privacy Law 224.
autonomy to choose and the digital personality should similarly not be restricted to specific online environments.\textsuperscript{13} Portability, in this sense, is intrinsically linked to broader notions of information privacy, as exemplified by Article 20 of the GDPR.

Article 20 creates a new right of data portability that goes beyond the access principles of traditional information privacy laws.\textsuperscript{14} Portability under Article 20 is primarily intended to empower individuals by providing them with more control over the transfer of their data.\textsuperscript{15} Under Article 20, a data subject can receive or transfer their personal data, provided to a data collector in digital format, in a structured, commonly used and machine-readable format for their own use.\textsuperscript{16} The data portability right encourages interoperability of data formats and the adoption of common data storage and data processing standards to facilitate porting.\textsuperscript{17} Article 20 has three components:\textsuperscript{18} access; reception and transmission that operate together to provide enhanced individual protections and also foster competitive opportunities. Data controllers are also required to transmit portable data to another controller without hindrance.\textsuperscript{19} Unhindered transfer reduces the types of locking-in concerns\textsuperscript{20} highlighted above and ameliorates corporate ownership of personal data thus reducing switching costs for individuals.\textsuperscript{21}

Article 20 does not extend to all circumstances and it does have limits in application. It only applies to personal data in digital formats provided to a data controller by an individual\textsuperscript{22} and it does not cover personal data acquired by the controller from other sources.\textsuperscript{23} It also

\textsuperscript{13} B Custers and H Uršic, 'Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection', (2016) 6 (1) International Data Privacy Law 4.
\textsuperscript{14} I Graef, M Husovec and N Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law', (2017) 3.
\textsuperscript{15} Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ 2016 L 119/1 at recital 68.
\textsuperscript{16} Uršic (n 7) 52-53.
\textsuperscript{17} Note, however, that Article 20 encourages rather than mandates interoperability.
\textsuperscript{18} B Van der Auwermeulen, 'How to Attribute the Right to Data Portability in Europe: A Comparative Analysis of Legislations', (2017) 33 (1) Computer Law & Security Review 57, 69.
\textsuperscript{19} General Data Protection Regulation, Art 20(1).
\textsuperscript{20} P Swire and Y Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique', (2013) 72 (2) Maryland Law Review 335, 336.
\textsuperscript{21} Graef (n 12) 59.
\textsuperscript{22} General Data Protection Regulation, Art. 20(1).
\textsuperscript{23} Article 29 Working Party, 'Guidelines on the Right to Data Portability' (WP 242 rev.01, 5 April 2017), 9.
does not apply when the data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, such as, when a data controller is exercising its public duties or complying with a legal obligation. The right also does not apply to portability in respect of profiling or analytics work undertaken by data controllers. Corporations can still safeguard their competitive advantage and intellectual property by retaining algorithmically-driven insights.

Despite the implementation of Article 20 within the broader rights based framework of the GDPR, some commentators previously expressed concern about elevating data portability mechanisms to the scope and application of fundamental rights. Critics of this approach argued that data portability should instead be considered as a narrower competition law mechanism. A greater emphasis is consequently placed on potential competition law objectives, such as the reduction of potential harms arising from ‘network effects’ and ‘vendor lock-in.’ Data portability schemes based on competition law principles seek to enable individual consumers and businesses to efficiently transfer and migrate their data between cloud and service providers, as well as foster new data-driven services and market entrants by permitting access to consumer data sets that had previously been monopolised by established market players.

Under a competition law perspective of data portability, network effects may also be viewed as a concern about social network platforms given the rapid scale of potential user spread by the innocuous action of ‘friending.’ A small network can grow quickly which can disproportionately extend the rapid reach of the platform to a much greater range of potential...

---

24 General Data Protection Regulation, Art 20(3).
25 Article 29 Data Protection Working Party, 'Guidelines on the Right to "Data Portability"' (n 23), 10.
26 Van der Auwermeulen (n 18) 799.
27 Swire and Lagos (n 20) 365.
28 Omer and Jules Polonetsky Tene, 'Big Data for All: Privacy and User Control in the Age of Analytics', (2013) 11 Northwestern Journal of Technology & Intellectual Property 239, 269.
29 I Graef, M Husovec and N Purtova (12) 4; A Daly and S Esayas, 'The Proposed Australian Consumer Data Right: A European Comparison', (2018) 3 European Competition and Regulatory Law Review 1, 7.
30 H Shelanski, 'Information, Innovation, and Competition Policy for the Internet', (2013) 161 (6) University of Pennsylvania Law Review 43, 1682-3; Swire (n 20) 359; I Graef, 'Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union', (2015) 39 (6) Telecommunications Policy 502, 503.
31 See Van Der Auwermeulen (n 18) 59; Zanfir (n 6) 152; Graef (n 12) 506.
32 Daly and Esayas (n 29) 10.
33 C Yoo, 'When Antitrust Met Facebook', (2012) 19 (5) George Mason Law Review 1147.
users. Rapid extension can then lead to the locking-in of service users especially where the financial, emotional, social and practical costs of switching service become too extensive.

A debate about the appropriate melding of information privacy and competition law regimes into portability frameworks thus unfolds, with some commentators critical of the role of information privacy law in data portability and others supportive.

Some commentators argue that information privacy and competition law frameworks are not readily compatible and thus one should take prominence over the other. The application of competition law remedies, predicated on misuses of market power or dominance, are undertaken on a case-by-case, harm analysis. However, data portability as a predominant information privacy mechanism, is constructed comprehensively, to apply to all organisations whether a harm emanates or not. Moreover, information privacy considerations are limited because of the ostensible focus on personal information which precludes anti-competitive behaviour that does not use such data. As Engels contends, care must therefore be taken to ensure that a melded mechanism does not unnecessarily stymie digital innovations by mandating comprehensive transfer procedures with minimally positive regulatory effect. It is argued that competition law principles thus override information privacy law considerations in the construction of portability mechanisms.

However, not all commentators see the complex relationship between information privacy and competition law as unsuitable for the development of a portability right. Both competition and information privacy perspectives essentially seek to augment consumer

34 B Engels, 'Data Portability Among Online Platforms', (2016) 5 (2) Internet Policy Review.
35 I Walden and L Da Correggio Luciano, 'Facilitating Competition in the Clouds' in C Millard (ed), Cloud Computing Law (OUP 2013) 311, 319; Article 29 Data Protection Working Party, 'Guidelines on the Right to "Data Portability" (n 23), 4; Graef (n 12) 506.
36 Engels (n 34) 4; A Diker and M Bilal Unver Vanberg, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?', (2017) 8(1) European Journal of Law and Technology 1, 14. Graef (n 12) 59.
37 Walden (n 35); Graef (n 12) 59.
38 Graef (n 12) 509; I Graef, J Verschakelen and P Valcke, 'Putting the Right to Data Portability into a Competition Law Perspective', (2013) The Journal of the Higher School of Economics 53, 57.
39 Swire (n 20) 352-3; Van der Auwermeulen (n 18) 61; Engels (n 34) 4; D Rubinfield and M Gal, 'Access Barriers to Big Data', (2017) 59 Arizona Law Review, 373.
40 Engels (n 34).
41 S Esayas, 'Competition in (data) privacy: ‘zero’-price markets, market power, and the role of competition law', (2018) 8 (3) International Data Privacy Law 181; I Graef, D Clifford and P Valcke, 'Fairness and enforcement: bridging competition, data protection, and consumer law', (2018) 8 (3) International Data Privacy Law 200.
42 Uršic (n 7) 59; Walden (n 35) 328.
trust around the use of personal information, albeit through different conceptual emphases.\textsuperscript{43} Recognising data portability as an individually focused right ameliorates some of the challenges of the competition law framework, which requires active emanation of harm.\textsuperscript{44} Data portability as an information privacy mechanism may therefore be a more ‘effective pro-competitive lever’ to address issues of locking-in, precisely because it does not require the challenging evidential requirements of market abuse.\textsuperscript{45} The fusion of competition and information privacy thus adds structural and individual protection within a portability framework.\textsuperscript{46} In effect, individual data use and control of personal information is the key driver of a successful portability scheme.\textsuperscript{47} Competition law policy implications are important, but are nonetheless, not the prime concern.\textsuperscript{48}

III. The CDR’s Policy Vectors

Section II highlights that data portability is a multi-faceted concept and it is important to illuminate the complex interplay of competition law and information privacy law considerations that underpin the implementation and operation of a data portability scheme. In this section, we identify three key policy vectors that are common to the CDR, its predecessors and pertinent, European and UK legal developments. The three vectors are: the scope of the proposed portability right in terms of regulated data; information privacy and security protections and the recommended regulatory framework. As will be evident from the sub-sections below, it is important to understand the CDR’s history as it overlaps significantly with UK, and therefore EU, developments. Moreover, the antecedents are important to comprehend in order to understand the differences in operation between the CDR and the Privacy Act, as outlined in Table 1.

\textsuperscript{43} A Rossi, H Feld and E Kimmelman, ‘The limits of antitrust in privacy protection’, (2018) 8(3) International Data Privacy Law 270, 274. Van der Auwermeulen (n 18) 59; Lynskey (n 6) 795.
\textsuperscript{44} Walden (n 35) 328.
\textsuperscript{45} Ibid 330.
\textsuperscript{46} Graef (n 12) 58.
\textsuperscript{47} Rossi, Feld and Kimmelman (n 43) 271.
\textsuperscript{48} Lynskey (n 6) 814; Graef (n 12) 59.
Table 1. Differences between the CDR and the Privacy Act across the three vectors

| Vector                      | CDR                                      | Privacy Act                                      |
|-----------------------------|------------------------------------------|--------------------------------------------------|
| Regulated Data              | CDR data that relates to a CDR consumer  | Personal information about an identified or reasonably identifiable person |
| Privacy and Security Mechanism | CDR Privacy Safeguards                  | Australian Privacy Principles                    |
| Regulatory Focus            | Prescriptive                             | Principles-based                                 |

A. **Regulated Data**

The CDR applies to consumer data in the banking, energy and telecommunications sectors, and mandates that prescribed ‘CDR data’ be made available for consumer access and transfer. The scheme is intended to be expanded on a sector-by-sector basis over time. At the timing of writing, the precise scope of the right in terms of portable data has only been determined for the banking sector, with both ‘customer-provided data’ and ‘transaction data’ to be made available for consumer access and transfer.

Earlier reviews and inquiries preceding the CDR considered different scopes of application. The Productivity Commission first recommended that regulated ‘consumer data’ should be determined by industry through a ‘data-specification agreement’ and registered with the Australian Competition and Consumer Commission (‘ACCC’). In the absence of industry agreement, the Productivity Commission recommended that regulated ‘consumer data’ should default to a ‘broad’ definition, including personal information as defined under section 6(1) of the Privacy Act, and other generally defined datasets. The OBR then...

---

49 Department of the Treasury (Cth), Consumer Data Right Booklet (9 May 2018), 3-4.
50 Ibid.
51 Open Banking Review (n 1) 33. Customer-provided data is data provided by customers directly to the banking institution. Transaction data is generated from transactions made on a customer’s account or service, and includes records of account balances, deposits, withdrawals, transfers, and the use of lending products such as mortgages, business finance, loans and credit cards.
52 Productivity Commission (n 2).
53 Ibid, 36.
54 Privacy Act 1988 (Cth) s 6(1): "Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable."
55 Productivity Commission (n 2) 36.
recommended that a ‘sector assessment’ process should be used to determine which datasets were subject to the portability right, involving input from the Federal Treasury, ACCC, Office of the Australian Information Commissioner (‘OAIC’), relevant sector regulators, consumers and industry.\textsuperscript{56}

The CDR retains the OBR’s recommendation that the Treasurer, as the minister responsible for competition policy, shall designate the sectors and datasets which will be subject to the portability right.\textsuperscript{57} The sector designation will be informed by the ‘sectoral assessment’ process conducted primarily by the ACCC and the OAIC, in consultation with industry, consumers and sectoral regulators.\textsuperscript{58} The assessment process is crucial. It effectively defines the scope of the CDR scheme in each sector and the datasets to be categorised as ‘CDR data’ by the Treasurer’s designation instrument under s56AC(2).\textsuperscript{59}

The CDR’s scope bears resemblance to consumer data portability schemes in the EU and UK. Specifically, the CDR’s sectoral coverage of banking data is comparable to the UK’s Open Banking scheme. The UK Open Banking scheme was initiated by the Competition Markets Authority (‘CMA’),\textsuperscript{60} and mandatorily requires nine of the largest banks in the UK to adopt standardised APIs facilitating the access and transfer of specified banking data, including transaction data. Both the CDR and UK Open Banking scheme take a prescriptive approach to defining the scope of data portable under each regime, such as ‘customer transaction data.’\textsuperscript{61}

To a lesser extent, the scope of the CDR is also similar to PSD2, which imposes a statutory requirement on banks to implement APIs allow for secure communication with third-party payment service providers and account information service providers.\textsuperscript{62} The APIs enable consumers and businesses to access and share transaction information with third party banks

\begin{itemize}
\item \textsuperscript{56} Open Banking Review (n 1) 17.
\item \textsuperscript{57} Treasury Laws Amendment (Consumer Data Right) Bill 2019, s 56AC.
\item \textsuperscript{58} Ibid ss 56AD, 56AE.
\item \textsuperscript{59} Ibid s 56AF(1).
\item \textsuperscript{60} Competition and Markets Authority (UK), Retail banking market investigation (26 February 2016); Competition and Markets Authority (UK), Retail Banking Market Investigation Order 2017 (2 February 2017).
\item \textsuperscript{61} Open Banking Working Group, The Open Banking Standard (April 2017), 17 <https://www.paymentsforum.uk/sites/default/files/documents/Background%20Document%20No.%202%20-%20The%20Open%20Banking%20Standard%20-%20Full%20Report.pdf>.
\item \textsuperscript{62} Payment Services Directive II Articles 66 and 67.
\end{itemize}
and FinTechs, and grant them read or write access over the customer’s transaction and banking data. Furthermore, the CDR’s future coverage of energy data, including smart meter data, is comparable to the interoperability requirements and procedures for access to smart meter data provided by the EU’s Common Rules for the Internal Market for Electricity.  

B. PRIVACY AND SECURITY PROTECTIONS

The CDR takes a unique approach to privacy safeguards, in that data transferred within the scheme, including personal information, is exempt from the operation the Privacy Act. This stands in stark contrast with comparable UK and EU consumer data portability legislation, for which the GDPR continues to apply to personal data transferred within those schemes.

Instead, the CDR scheme includes a separate, stand-alone set of ‘CDR Privacy Safeguards’ for both personal information and ‘CDR data’ transferred in the scheme. The CDR Privacy Safeguards govern third parties who receive data within the CDR scheme, including when and how they may collect, use and disclose CDR data, as well as obligations pertaining to data quality and security. The CDR Privacy Safeguards largely replicate the Privacy Act’s Australian Privacy Principles (APPs) in terms of their regulation of the data processing lifecycle.

This position would be in line with portability laws in the UK and EU. Whilst PSD2 and the UK Open Banking regime in some areas set more specific and stricter standards than the GDPR around consent and technical security standards for APIs, the GDPR provides the foundational data protection safeguards. Individuals can still freely exercise their GDPR rights in relation to personal data transferred through PSD2 or the UK Open Banking Scheme.

Indeed, one challenge with portability schemes is that additional privacy and security requirements may need to be specified such as technical security standards for mandated

---

63 EU Internal Electricity Market Directive, Articles 11, 12, 21, 23, 24. see also, Daly and Esayas (n 7), 18-19.
64 Payment Services Directive II, Article 67(2)(f).
65 Treasury Laws Amendment (Consumer Data Right) Bill 2019, Division 5, Privacy Safeguards.
66 Payment Services Directive II, Article 94(2); see also, S Mezzacapo, 'Competition policy issues in EU retail payment business: the new PSD 2 regulatory principle of open online access to information from "payment accounts" and associated "payment transactions", (2018) 39 European Competition Law Review 534, 541.
67 Article 67(2)(f) PSD2.
APIs, or consent requirements for corporate entities utilising the scheme. This is the approach undertaken in the CDR as it replaces the operation of the *Privacy Act* with its CDR Privacy Safeguards, rather than supplementing the *Privacy Act*. It effectively implements a new information privacy law regime to obviate the challenges of entity and data categorisation arising from the *Privacy Act*. As detailed below, the replacement of the *Privacy Act* presents challenges in managing the interoperation of the *Privacy Act* and CDR Privacy Safeguards.

C. **REGULATORY FRAMEWORK**

The CDR will be administered by multiple regulators, most prominently, Australia’s competition law and privacy law authorities, namely the ACCC and OAIC. In a way, this reflects the competing policy tensions at the centre of data portability schemes, highlighted at Section II above.

The ACCC will be the principle rule-setting regulator and will draft sector-specific CDR Rules for each new sector in which the portability right will be applied. The CDR Rules cover the scope of portable ‘CDR data’ in each sector, accreditation requirements and process, the substantive content of the CDR Privacy Safeguards and technical data security requirements, among other things. In this regard, the ACCC will act as ‘lead regulator’ who will hold the ‘primary responsibility’ for systemic compliance. The ACCC will be required to consult with the OAIC in the process of drafting sector-specific rules. The OAIC will have principal responsibility for privacy protection and is the primary complaint handler for individual information privacy complaints.

The proposed multi-regulator model appears to have been heavily influenced by the UK Open Banking Regime. The law reform process explicitly referenced the UK Open Banking Regime as a model for setting out regulator responsibilities over the CDR scheme. In the UK, the Competition and Markets Authority (CMA) issued the direction that required the

---

68 See Open Banking Review (n 1), 54.
69 Explanatory Materials, Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Exposure Draft) 30.
70 Ibid.
71 Ibid.
72 Ibid.
73 Open Banking Review (n 1) 17.
implementation of Open Banking, the Financial Conduct Authority (FCA) is responsible for third party accreditation and the administration of PSD2, and the Information Commissioner’s Office remains responsible for data protection under the GDPR. The CDR’s adoption of technical standards and data recipient accreditation were also adopted with explicit reference to the UK Open Banking scheme.

IV. **AN UNCERTAIN ROLE**

The comparison of the CDR with its Australian policy predecessors and its UK and EU counterparts is important to understand. As Section III notes, the CDR flows from both the OBR and the Productivity Commission’s analysis and thus inherits many of the competition-enhancing purposes of the UK Open Banking scheme. These points are important because the analysis begins to shift towards the complex interrelation between competitive policy priorities and the role of information privacy law frameworks in the implementation and application of the CDR’s overarching competition law policy aims. We now demonstrate in this section, the uncertain role for Australian information privacy law in relation to the overall operation of the CDR. To do so, we return to the fundamental nature of a data portability scheme and the complexities inherent in the amalgam of information privacy law and competition law. It is here where the uncertain role of the Australian information privacy law regime under the CDR becomes evident. The antecedent history of the CDR is important in this regard because it sheds light on policymaker perspectives regarding the overall veracity of the *Privacy Act* and its ability, or inability, to be an implementation vehicle that enhances consumer trust in portability.

We contend that the CDR’s approach to information privacy is problematic when examined against the three policy vectors identified in Section III. First, the adopted definitions of CDR data and CDR consumer, and thus the whole scope of the CDR, sits uncomfortably alongside the definition of personal information under the *Privacy Act*. Second, the CDR scheme could create duplication of information privacy regulatory requirements that are dependent on the complex ‘switching on and off’ mechanism of the CDR Privacy Safeguards. Third, the

---

74 Ibid xvii.
75 Ibid 22.
regulatory framework adopted is potentially problematic as the CDR scheme seeks to incorporate both principles-based and prescriptive rules for privacy protections. Moreover, the privacy regime will be determined in large part by the ACCC, a regulator whose expertise is not in information privacy law matters.

A. REGULATED DATA: DEFINITIONAL PROBLEMS

Section III.A noted that the CDR’s implementation strategy creates a complex interplay of different legislative and regulatory requirements that entail several foundational definitions, especially in relation to CDR data and personal information. The application of these foundational definitions is currently uncertain particularly regarding the issue of whether transaction data constitutes personal information under the Privacy Act, following the case of Privacy Commissioner v Telstra.76

In Telstra, the Full Court of the Federal Court of Australia was asked by the Privacy Commissioner to consider the statutory relevance of ‘about’77 in the previous definition of personal information.78 The case involved a protracted dispute between the journalist, Ben Grubb, and his mobile service provider, Telstra about accessing mobile metadata. Telstra provided some data but declined Grubb’s access request in relation to location-based cell tower data. Even though it regularly provided such data for law enforcement agencies upon request, Telstra argued it was unreasonable for an individual access request because it was too complicated, time-consuming and expensive.79

Grubb complained to the Privacy Commissioner and the Commissioner decided that the location metadata was personal information because Grubb could be identified in a reasonably ascertainable sense.80 The Commissioner’s decision relied heavily on the VCAT decision, WL v La Trobe (WL),81 which indicated the practical boundaries of reasonably ascertainable categorisation.82 Both the Commissioner’s decision and WL are predicated on a

76 The Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 (19 January 2017).
77 Ibid [5] per Kenny and Edelman JJ.
78 The key part of the previous definition being ‘apparent or reasonably ascertainable.’
79 Ben Grubb and Telstra Corporation Limited [2015] AICmr 35 (1 May 2015), [86].
80 Ibid [93]-[102].
81 Ibid [56]-[57], [70]-[71].
82 WL v La Trobe University (General) [2005] VCAT 2592 (8 December 2005) [42] per Coghlan Deputy President (DP).
certain logic regarding the identification of data that is personal information. If an individual’s identity is apparent or reasonably ascertainable, or under the current definition, identifiable or reasonably identifiable, then data should be deemed to be about an individual and be classed as personal information. ‘About,’ in this sense, gets its statutory application from the notion of identity which, at the time, was generally settled law based on WL.\textsuperscript{83}

That categorisation process was then turned upside down on appeal to the Administrative Appeals Tribunal (AAT).\textsuperscript{84} Tribunal Deputy President Forgie determined the threshold question to be whether the cell tower data was about an individual which entailed the ‘subject matter’ or character of information.\textsuperscript{85} It is now necessary to determine that the subject matter of any given piece of information is about an individual. If it is not, then ‘that is the end of the matter’\textsuperscript{86} and it does not matter whether identification can be determined from that information, either in an apparent, or in a reasonably ascertainable sense.\textsuperscript{87}

The AAT decision set the scene for the Privacy Commissioner’s appeal to the Federal Court. It should be noted that, rather bizarrely, the Commissioner’s ground of appeal was not the basis of his original decision, namely, the cell tower metadata was personal information. Instead, the issue put forward for adjudication was whether ‘about’ in the definition of personal information had substantive application.\textsuperscript{88} The confused Court\textsuperscript{89} could therefore only adjudicate on the very narrow question of whether ‘about’ has statutory purpose, rather than the more pressing question of when metadata can be constituted to be personal information in a reasonably ascertainable sense. Not surprisingly, the Court held that ‘about’ had substantive application and partially affirmed the logic of the AAT decision.\textsuperscript{90}

The Federal Court also broadened the scope of the AAT decision by accepting that information can have ‘multiple subject matters’ and thus ‘an evaluative conclusion’ is

\textsuperscript{83} Ben Grubb and Telstra Corporation Limited [2015] AICmr 35 (1 May 2015), [81]-[83].
\textsuperscript{84} Telstra Corporation Limited and Privacy Commissioner [2015] AATA 991 (18 December 2015).
\textsuperscript{85} Ibid [98].
\textsuperscript{86} Ibid [95].
\textsuperscript{87} Ibid [97].
\textsuperscript{88} The Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 (19 January 2017 [5].
\textsuperscript{89} Ibid [80].
\textsuperscript{90} Ibid [63], [65].
required that considers information in its totality.\textsuperscript{91} Even though one piece of information may not be about an individual, it can become so when aggregated with other information. However, the Court did not indicate when, and in what circumstances, information can have multiple subject matters, and more importantly, when a multiple subject matter characterisation can be about an individual in the context of identification under the old definition of s6(1).

The result of this litigation is that while it is highly likely that customer provided data will be personal information, it is currently unclear whether, and in, what circumstances transaction data, including metadata ported under the CDR, would be personal information. If that is the case, then the same challenges may arise for the application of information privacy protections accorded via the \textit{Privacy Act}. Unless the definition of personal information is amended in the \textit{Privacy Act}, it would be difficult to implement the privacy elements of a portability scheme, including the CDR, entirely through that law.

It is perhaps this background that helps to explain the different approach adopted in the CDR. CDR data will ultimately be designated by an ACCC regulatory instrument and will include a range of data relevant to natural persons and corporations.\textsuperscript{92} It will constitute three general categories: data that relates to a CDR consumer or has been provided by one that includes transaction data; data that relates to a product and data derived from primary sources.\textsuperscript{93} It is immediately clear that the definition of CDR data incorporates the foundational ‘relates’ element of personal data in the GDPR rather than ‘about’ in the \textit{Privacy Act}. The CDR Explanatory Memorandum states why:

\begin{quote}
CDR data is data that ‘relates’ to a CDR consumer. The concept of ‘relates to’ is a broader concept than information ‘about’ an identifiable or reasonably identifiable person under the Privacy Act. The term ‘relates’ has a broader meaning than ‘about’
\end{quote}

\textsuperscript{91} Ibid [63].
\textsuperscript{92} Explanatory Materials, Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Exposure Draft), 13 [1.50].
\textsuperscript{93} Ibid 13 [1.51].
and is intended to capture, for example metadata of the type found not to be about an individual in *Privacy Commissioner v Telstra Corporation Ltd*...94

The CDR seeks to explicitly avoid some of the definitional challenges caused by the *Telstra* case by having a more expansive definition of CDR data than personal information under the *Privacy Act*. A greater amount of data, particularly transaction data, can be definitively classed as CDR data that can then be ported. Once in the portability transfer system, the CDR Privacy Safeguards are switched on and then a different definition of CDR data applies, namely, ‘data in relation to a product and includes customer data, account data, transaction data and product data.’95 Customer data is then defined as ‘data that identifies a consumer and any persons authorised to act on the consumer’s account,’96 including identifying information to distinguish one consumer from another.97 Once in the system, the broader legislative definition of CDR data is then re-constituted into four other types of data that nevertheless could be classed as personal information in either a ‘relate’ or an ‘about’ sense.98

We believe that the use of ‘relates’ for the CDR scheme will give rise to problems within the broader Australian information privacy law framework. It will eventually create two separate jurisprudential tracks of reasoning regarding the type of data that will be covered under the CDR scheme and the broader ambit of the *Privacy Act*. The definitional use of ‘relates’ is specifically tied into the rights-based framework of privacy protections in the GDPR and the EU more generally.99 More data thus falls under the ambit of the GDPR as a policy counterpoint to the increasingly widespread use of data aggregation strategies.100 The use of ‘about’ in the *Privacy Act* was specifically designed to curtail the widespread application of the Act and confine it to a reduced range of information, to create certainty

---

94 Explanatory Materials, Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Exposure Draft, Second Stage) 10.
95 ACCC, ‘CDR Rules Outline’ (2018) <https://www.accc.gov.au/focus-areas/consumer-data-right/rules-outline>, [4.1].
96 Ibid [4.12].
97 Ibid [4.13].
98 The multiple definitions of CDR data has been a point of criticism. OAIC, ‘Consumer Data Right (CDR) exposure draft legislation — submission to The Treasury’ (September 2018).
99 General Data Protection Regulation, Recitals [1]-[3]; Article 29 Data Protection Working Party (n 59), 4.
100 European Data Protection Supervisor, ‘EDPS recommendations on the EU’s options for data protection reform’ (2015); Article 29 Data Protection Working Party, ‘Opinion 8/2014 on the Recent Developments on the Internet of Things’ (WP 223, 16 September 2014); Article 29 Data Protection Working Party (n 59).
and minimise the regulatory load on regulated entities.\textsuperscript{101} It was some of these general points of statutory interpretation that formed the AAT decision\textsuperscript{102} which appear to receive tacit support in the Federal Court’s decision in the \textit{Telstra} case.\textsuperscript{103}

The broader definition of CDR data is specifically designed to avoid the problems arising from the \textit{Telstra} case to ensure that more data, particularly transaction data, is ported through the scheme. The recognition of the competition law perspective is important here because the information privacy element of the scheme is being utilised to stimulate data transfer practices for the benefit of the wider digital economy. In so doing, the broader definition of CDR data provides added individual benefit and attempts to raise levels of consumer trust in the operation of the system, in conjunction with the CDR Privacy Safeguards.

We contend that these definitional tensions will be difficult to reconcile for regulated entities. The emphasis on consumer and privacy trust building in the CDR scheme should not be undertaken at the expense of critically examining the basis and effectiveness of the broader information privacy law framework, as noted by the OBR. Instead, we argue that consideration ought to have been paid to the limitations of the current definition of ‘personal information’ in the \textit{Privacy Act}, and that the \textit{Privacy Act} should have been amended to cover data that ‘relates’ to an identified or reasonably identifiable individual, bringing it in line with the GDPR. Without doing so, we reach the incoherent outcome where metadata transferred in the CDR scheme will be protected by the CDR Privacy Safeguards when they are ‘switched on’ for accredited data recipients, but if and when the CDR Safeguards ultimately ‘switch off’, metadata will not be protected under the \textit{Privacy Act}.

It should also be borne in mind that the implementation of Article 20 of the GDPR also came in tandem with a suite of protective enhancements including the development of previously existing, fledgling ‘micro-rights.’\textsuperscript{104} That is not the case with the CDR bill where the information privacy elements are centred upon the delivery of an ostensible competition law mechanism as a trust enhancement process to the potential detriment of the wider Australian

\begin{flushright}
101 Australian Law Reform Commission, \textit{For Your Information: Australian Privacy Law and Practice} (Law Reform Commission, 2008), 306.

102 Ibid; \textit{Telstra Corporation Limited and Privacy Commissioner} [2015] AATA 991 (18 December 2015), [35], [98].

103 \textit{The Privacy Commissioner v Telstra Corporation Limited} [2017] FCAFC 4 (19 January 2017), [41].

104 Lynskey (n 6) 809.
\end{flushright}
privacy framework. We therefore argue that an amended Privacy Act ought to have been used as the vehicle to deliver privacy protections for data transferred within the CDR scheme, as exemplified by the potential duplication issues arising from the ‘switching process.’

As noted below, and in the antecedent inquiries to the CDR, this is not a simple task as the Privacy Act has been continually criticised for its lack of substantive individual protections. The definition of personal information is a case in point given its deliberately constrained application. However, we do not believe these deficiencies should not have precluded the implementation of the CDR through the Act. Instead, rather than avoiding the weaknesses of the Privacy Act, implementing the CDR through the Act would have turned critical attention to the overall veracity of Australia’s privacy law framework and its ability or inability to sustain ongoing digital developments. Such attention was recently provided by the ACCC in its Digital Platforms Report which called for the further strengthening of the Privacy Act and the overarching Australian privacy law framework.105 The report recommended a greater alignment with recent international developments, including the GDPR, which would require a change in the definition of personal information.106 All of this would seem to suggest that the Privacy Act could be sufficiently updated thus avoiding the requirement for an ancillary CDR structure.

B. PRIVACY AND SECURITY PROTECTIONS: Duplicated Obligations?

Along with definitional challenges, we further argue that the CDR Privacy Safeguards will potentially lead to duplicated privacy obligations. The Safeguards are modelled on the APPs because they regulate how a data collector, in this case ‘accredited data recipients’, must treat information throughout the lifecycle of personal information processing, including collection, storage, use and disclosure. Given that the CDR Privacy Safeguards impose similar obligations to the APPs, there is a risk that two information privacy frameworks will overlap in their application to the same datasets.107 Overlapping privacy obligations could

105 ACCC, ‘Digital Platforms Report’ (2019). See specifically Chapter 7 and conclusions.
106 Ibid. 460.
107 OAIC, ‘Consumer Data Right (CDR) exposure draft legislation — submission to The Treasury’ (September 2018); Law Council of Australia, ‘Submission to Exposure Draft - Treasury Laws Amendment (Consumer Data Right) Bill 2018’ (September 2018) <https://www.lawcouncil.asn.au/resources/ submissions/exposure-draft-treasury-laws-amendment-consumer-data-right-bill-2018>, 4.
lead to regulatory inefficiencies, confusion on part of regulated entities, and higher compliance costs for regulated entities.

The CDR scheme attempts to avoid the duplication of privacy obligations through a complex interplay of switching mechanisms, in which the APP obligations under the Privacy Act ‘switch off’ once a portability transfer commences, and the CDR Privacy Safeguards then switch on. Rather than being duplicated processes, it is contended by the CDR’s drafters that both the APPs and the Privacy Safeguards work in tandem when switched on and off at separate times in the overall process of portability. However, the exact scope of the switching mechanism is unclear.

For example, as noted above, the CDR framework relies on a complex interplay of different legislative and regulatory requirements. These operate to different classes of participants in the CDR system, namely, data holders and accredited data recipients. Broadly, the Privacy Act applies to data holders and the CDR Privacy Safeguards apply to the accredited data recipients. A ‘data holder’ is defined as a party who holds CDR data on behalf of a person, and is either: (i) specified in a sector designation instrument; (ii) a data holder by virtue of the principle of reciprocity; or, (iii) a data holder by virtue of a condition in the Consumer Data Rules. The first of these alternatives is likely to be the most common. For example, in an open banking context, data holders would be Authorised Deposit-taking Institutions (ADIs), as specified in the designation instrument, and would typically be a consumer’s current bank. By contrast, an ‘accredited data recipient’ is a party who has been disclosed CDR data, under the CDR rules, and is not a data holder. Again, in the open banking context, the accredited data recipient could therefore be a third-party bank to whom the consumer wishes to switch to, or a third-party fintech who can offer new services using CDR data.

108 Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) 51-52.
109 Explanatory Materials, Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Exposure Draft, Second Stage) 13, [1.73]-[1.74].
110 Treasury Laws Amendment (Consumer Data Right) Bill 2019 s 56AG(1).
111 Ibid s 56AG(2)-(4).
112 Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2018 (Exposure Draft) s 5.
113 Treasury Laws Amendment (Consumer Data Right) Bill 2019 s 56AGA.
When a transfer request is lodged, the APPs ‘switch off’ for the data holder (e.g. the customer’s original bank) who must then comply with the Privacy Safeguards when transferring the CDR data to the customer’s chosen accredited data recipient. The accredited data recipient must then handle and process the transferred CDR data in accordance with the Privacy Safeguards, and not the APPs.\textsuperscript{114} For example, under the Privacy Safeguards, the accredited data recipient (e.g. a fintech or bank) may only use and disclose the received CDR data\textsuperscript{115} in accordance with the CDR consumer’s express, purpose-limited and time-limited consent\textsuperscript{116} given when submitting the transfer request. The consumer’s consent, which sets the permissible uses and disclosures of their CDR data, automatically expires after a period of 12 months,\textsuperscript{117} though the CDR Standards are likely to provide for a simple process of renewing consent.\textsuperscript{118} However, any new CDR data or personal information collected or generated by the accredited data recipient must, by contrast, be treated in accordance with the APPs.\textsuperscript{119} Figure 1 details the porting process for Data Holders and Accredited Data Recipients under the CDR.

Figure 1. Porting process under the CDR

\begin{itemize}
\item Use/disclose in accordance with CDR Privacy Safeguards.
\item Prescriptive, time-limited and purpose-specific consents managed through CDR dashboards.
\item Use/disclose in accordance with Privacy Act.
\item Use/disclose according to notified primary purposes or reasonable expectations of the individual.
\end{itemize}

\textsuperscript{114}Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth), s 56EC(4)(a).
\textsuperscript{115}Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth), s 56El(1)(b); ACCC, ‘Consumer Data Right Rules Outline’, (December 2018), 8.8 [26].
\textsuperscript{116}ACCC, ‘Consumer Data Right Rules Outline’, (December 2018), 7.10 [21].
\textsuperscript{117}ACCC, ‘Consumer Data Right Rules Outline’, (December 2018), 7.25 [24].
\textsuperscript{118}Ibid, 7.27 [24].
\textsuperscript{119}Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth), s 56AJ(3); see also, Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth), 1.83 [18].
Figure 1 outlines that accredited data recipients will have to navigate two privacy frameworks in managing a single consumer’s data – the Privacy Safeguards for CDR data received through a CDR scheme transfer, and the APPs for CDR data or personal information collected or generated itself after the transfer. Regulated entities will therefore be required to implement a two-tiered risk management process to comply with both information privacy regimes.

The CDR does outline the possibility that certain accredited data recipients may have their information privacy obligations switch wholly back to the APPs at some stage following a transfer (including for received CDR data), depending on the conditions laid out in the CDR Rules. The OAIC’s submission on this point observed that there is a lack of certainty and clarity around the boundaries of the CDR scheme and the CDR privacy safeguards.

The likely result is that despite the ‘switching on and off’ mechanism, there will be a significant degree of overlap of privacy obligations for accredited data recipients. Even if the ACCC creates conditions in the CDR Rules to the effect that some accredited data recipients ultimately ‘switch back’ to being wholly regulated by the APPs, in practice, these organisations will have to obtain advice as to the application of both privacy regimes and both sets of privacy principles. The fact that this switching mechanism will take place between prescriptive and principles-based privacy obligations may further complicate the two-track compliance process, as detailed below.

Instead of the switching mechanism, we again argue that the Australian information privacy law framework is the more appropriate vehicle to determine and govern privacy obligations, as it is a regime designed for this purpose. The CDR’s envisaged role of information privacy law, on the other hand, appears to be solely as a consumer trust enhancement mechanism. Information privacy law, in this sense, is not treated as a fundamental statutory or

---

120 Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth), 1.85 [18]:
121 Ibid, 1.83 [18].
122 Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth), s 56A(4); see also, Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth), 1.86-1.87 [19]
123 OAIC (n 134).
124 Ibid.
125 Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth), 1.88 [19].
126 OAIC (n 107).
constitutional right. Instead, it is treated as a perfunctory part of regulatory rules which are the ‘primary mechanism through which consumers and their data are protected.’\textsuperscript{127} The CDR approach to information privacy law again points towards a dominant regulatory perspective squarely focussed on competition law imperatives which points critical attention towards the regulatory framework adopted.

C. REGULATORY FRAMEWORK: CONCEPTUALLY DIFFERENT STRUCTURES

The above issues are amplified due to the underpinning regulatory structures that govern the APPs and the Privacy Safeguards rely on different conceptual bases. The Privacy Act is based on a principles-based regulatory (PBR) mechanism and the CDR Privacy Safeguard are prescriptive in nature. As highlighted above, the utility of these parallel regimes is largely dependent on the efficacy of the switching process. However, given the significant differences in regulatory aims between the Privacy Act’s PBR-based and the CDR’s prescriptive mode of operation, it is difficult to contemplate the smooth switching processes envisaged in the CDR.

The PBR basis of the Privacy Act provides a significant degree of leeway to the implementing bodies about how regulatory values and guidelines are implemented.\textsuperscript{128} The logic of delegated regulation provides that regulated entities have a better sense of effective coalface implementation compared to distant regulators.\textsuperscript{129} Regulatory requirements can be more finely attuned to meet broad legislative principles, particularly in fast moving areas of continuing technological development.\textsuperscript{130} As the primary privacy regulator, the OAIC sets guidelines on how the APPs should be interpreted and implemented within regulated entities.\textsuperscript{131} These guidelines provide minimum levels of regulatory expectation that fulfils a dual micro and macro purpose. First, the guidelines can be tailored by regulated entities to

\textsuperscript{127} Ibid, 6, quoting Explanatory Materials, Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Exposure Draft) [1.163].

\textsuperscript{128} Ibid, [4.16]-[4.17].

\textsuperscript{129} J Black, M Hopper and C Band, ‘Making a Success of Principles-Based Regulation’ (2007) 1 (4) Law and Financial Markets Review 191, 192.

\textsuperscript{130} Australian Law Reform Commission (n 203), 354, [4.93].

\textsuperscript{131} OAIC, ‘Australian Privacy Principles guidelines’ (2014); OAIC, ‘Guide to developing an APP privacy policy’ (2014); OAIC, ‘Guide to privacy regulatory action’ (2015); OAIC, Notifyable Data Breaches <https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/>. See also Black’s concerns with regulatory guidance in Black, Hopper and Band (n 129) 198.
meet individual circumstances. Second, the guidelines establish a broad-based implementation of minimum standards to guide regulatory activities predicated upon the openly semantic nature of principles-based construction. PBR schemes consequently provide a degree of trusted and guided detachment from the state.\textsuperscript{132}

Prescriptive schemes, such as the Privacy Safeguards, are predicated on the opposite. The state, in the form of its regulators, mandate the regulatory requirements to be fulfilled by regulated entities. Guidelines aimed at establishing an ongoing regulatory dialogue between regulators and regulated entities\textsuperscript{133} are replaced by rules that are promulgated at the discretion of the ACCC and must be followed to obviate punishments, such as, accreditation revocation\textsuperscript{134} or the imposition of civil penalties.\textsuperscript{135} There is no trusted detachment accorded by the state regarding the implementation of a prescriptive scheme.

A core concern with the two-track CDR scheme emerges. The two tracks entail identically structured principles and safeguards, but they do so from different underpinning regulatory structures. As outlined above, the potential for regulatory overlap is significant because CDR data holders and accredited data recipients will need to fulfill different regulatory roles across two different regulatory structures. The same data whether it be classed as CDR data or personal information will be regulated by similarly structured principles and rules. However, the data will be regulated in different ways, especially regarding the complex relationship between regulated entity and regulator(s). The two underpinning regulatory logics are seemingly incompatible in the context of the CDR. Under the APP application, regulated authority is delegated down, but is then taken away at the point of CDR portability when the Privacy Safeguards switch on. As noted above, this will lead to confusion on the part of regulated entities, who must switch between accorded discretion to implement broad privacy principles and following specifically prescribed rules and standards.

The justification for these potential incompatibilities appears to be a twofold argument. First, the CDR switching process will ameliorate or remove the possibility of duplication in the

\textsuperscript{132} J Black, ‘Forms and paradoxes of principles-based regulation’ (2008) 3 (4) Capital Markets Law Journal 425, 431.
\textsuperscript{133} Ibid 432.
\textsuperscript{134} Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth), s 56BH(1)(e).
\textsuperscript{135} Ibid s 56EU.
two-track approach. Second, rules are required to establish clear regulatory application to support the overall enhancement of consumer trust in the CDR’s privacy framework. We have difficulty with both justifications.

The CDR switching mechanism is unlikely to be a binary process in real world application. The application of different legislative and regulatory definitions will mean that CDR data will be concurrently captured under both the Privacy Act and the CDR scheme. However, the capture will be overlapping as some data will be covered by both frameworks, but other data will only be covered by the CDR scheme. That itself is not a problem if the switching mechanism works cleanly.

Our concern arises because the two-track approach will produce a veneer effect across both frameworks due to the ‘relates to’ definition inherent in CDR data. The veneer essentially spreads the intended GDPR rights-based underpinning of ‘relates to’ across both frameworks principally for the capture of CDR data. While it fulfils the pragmatic requirement of obviating confusion caused by the Telstra case, it does so by further weakening the comprehensive application of the Privacy Act and its own definition of personal information. The overall coherent application of Australia’s information privacy law framework is potentially being weakened for the basis of consumer trust enhancement in the CDR. Cohesive erosion will involve difficult regulated entity decision-making about compliance with both frameworks. At that point, regulated entities are going to be faced with challenging choices.

Two polar policy effects are going to operate at the same time, on the same sets of data. The CDR polar effect will mean that a large amount of CDR data that is unlikely to be classified as personal information under the Privacy Act, will nonetheless, be consumer data under the CDR and will entail Privacy Safeguard requirements during portability. The Privacy Act polar effect will mean a lesser amount of data will be classed as personal information, but protections will apply on that data for a much broader length of time under the application of the APPs. The regulatory residue that falls between those two polar policy effects is likely

---

136 Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) 9-10.
137 Department of the Treasury (Cth), ‘Consumer Data Right Privacy Protections Summary’ (September 2018) <https://treasury.gov.au/consultation/c2018-t316972/>. 

Electronic copy available at: https://ssrn.com/abstract=3699222
to be significant. Data holders will have to apply two sets of definitional considerations to essentially the same data sets in order to fulfil two different regulatory purposes with conflicting aims. CDR data is defined expansively and utilised narrowly in portability transfer. Personal information for APP coverage is defined narrowly but is utilised expansively.

We argue that the switching mechanism will really be a negotiated process of legal risk management within regulated entities rather than a binary and technical ‘flick a switch’ solution to avoid regulatory duplication. The switch may rightly be flicked at the portability stage, but the pre-flick entity discussions required to fulfil switching will be significant and challenging. The switching process begins way before the actual portability transfer of CDR data, and it is in this space where the residual regulatory effects of will require careful choice of legal risk management decision-making.

The second problem with the underpinning regulatory framework regards the roles played by the ACCC and the OAIC. The ACCC will be the ‘principal’ regulator for the CDR and the OAIC has a subordinate advisory role in relation to privacy matters. The claimed necessity of the CDR Rules is to enable the scheme to be flexible enough to be applied in different sectors.

Ideally, the OAIC should hold the primary rule-making responsibility in relation to the Privacy Safeguards. The OAIC is the regulatory body that has expertise in information privacy matters, whereas the ACCC has been established on a different conceptual basis, namely the promotion of competitive markets and consumer welfare. It is likely that the ACCC was chosen as the lead-rule maker due to the well-known passivity of the OAIC138 largely due to its chronic underfunding.

We argue that the OAIC should be appropriately funded and be given a statutory remit appropriate for the lead regulator of the CDR’s privacy aspects. As noted by the OBR, “a clearly focussed, accountable privacy advocate is a necessary element in a customer directed

---

138 J Signato and M Burdon, 'The Privacy Commissioner and Own-Motion Investigations into Serious Data Breaches: A Case of Going through the Motions?' (2015) 38 (3) University of New South Wales Law Journal 1145.
data transfer system.”¹³⁹ We agree with the OBR’s observations that the OAIC should be the primary rule-maker for privacy matters, to ensure that the Privacy Safeguards align coherently with the APPs. However, as outlined above, the current weaknesses of the Privacy Act should be ameliorated and this also includes a critical analysis of the role and funding regime of the OAIC. Doing so, would mean that data portability is no longer considered under the regulatory perspective of competition law. Instead, it would be part of a strengthened and coherent approach to information privacy law.

V. CONCLUSION

Our paper outlines issues that are likely to arise from the advent of the CDR regarding the intertwining of different definitions, potential duplicated privacy obligations and conceptually different regulatory schemes. We believe it would have been preferable to have the privacy aspects of the CDR governed by the Privacy Act, as per the Productivity Commission and OBR recommendations. There are concerns about the Privacy Act, but these should not be eschewed by the implementation of the CDR scheme. Those concerns should be addressed in order to bring the Privacy Act in line with the GDPR. This approach would have been conceptually clearer than the CDR Privacy Safeguards, as the Privacy Act is a regime designed for the purpose of providing privacy and security protections, and it would apply enhanced protections comprehensively.

A larger concern thus permeates our analysis and arguments. The complex policy considerations underlying data portability demonstrate the lack of a core understanding of information privacy law in the Australian policy context. The narrow construction of Australia’s data portability scheme, as an ostensible competition law mechanism, exemplifies this point. The CDR framework is not constructed around the type of data protection and broader privacy framework that underlies Article 20 of the GDPR, the UK Open Banking scheme or the EU’s PSD2. Instead, the CDR is designed as a hybrid of different elements, as an expeditious means to overcome foundational weaknesses in the Australian approach to information privacy law and privacy in general.

¹³⁹ Open Banking Review (n 1) 36.
This is a much deeper problem that goes beyond the appropriate construction of a data portability scheme. Without a core jurisprudential understanding of what privacy means, there is a distinct possibility that two separate tracks of judicial interpretation could emerge that mirrors the different statutory purposes of both schemes. If so, it is likely that the judicial categorisation of data types in both schemes will depart in different directions which could further weaken the already limited coherence of the *Privacy Act’s* comprehensive focus.

We contend that the CDR is absent a core understanding of what privacy is in Australia. The CDR concerns we highlight regard the reinforcement of Privacy Safeguards in the CDR at the expense of the relatively limited privacy protections in the APPs. We think this is the wrong approach. Privacy should be critically considered on its own merits rather than as a necessary function of data portability. In other words, privacy is not a bolt-on. Instead, it is a foundational protection that requires careful consideration, including in a competition law focussed data portability scheme.