UNSW Law & Justice Research Series

A World-Leading Sanitation System For Our Digital Economy: The Consumer Data Right

Natalia Jevglevskaja and Ross Buckley

[2023] *UNSWLRS* 6
Forthcoming in *Australian Business Law Review*

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

FORTHCOMING *AUSTRALIAN BUSINESS LAW REVIEW*

A WORLD-LEADING SANITATION SYSTEM FOR OUR DIGITAL ECONOMY: THE CONSUMER DATA RIGHT

Natalia Jevglevskaja[*]

Ross Buckley[**]

Sanitation engineers have saved far more human lives than doctors. The Consumer Data Right ('CDR') regime introduced in Australia in 2019 is a 'water supply and sanitation system' for Australia's digital economy. It provides the pipes through which data will flow securely, and ensures that waste data is disposed of safely. Thinking of the CDR in these terms provides a useful analogy for understanding the regime's pivotal role in driving innovation and competition in Australia while rigorously protecting consumer data and ensuring the system's trustworthiness. We currently have the only data-sharing regime in the world that extends beyond banking to other sectors. Yet few of us appreciate how far ahead we are of other nations, and how imperative it is that we continue to build on this lead.

1. Introduction

'Data is the new oil'. This quote is ubiquitous because it is both telling and true: oil powered economies in the 20th century, and data is powering them in the 21st century. Of the five most profitable companies in the world last year, two were oil companies and three were data companies – the trend is clear.[1]

[*] Natalia Jevglevskaja is a Research Fellow on the ARC Laureate Project on the data revolution at UNSW Sydney. Email: n.jevglevskaja@unsw.edu.au.

[**] Ross P Buckley is the KPMG Law - King & Wood Mallesons Professor of Disruptive Innovation, an Australian Research Council Laureate Fellow, and a Scientia Professor at UNSW Sydney. Email: ross.buckley@unsw.edu.au.

The authors gratefully acknowledge the financial support of the ARC Laureate Fellowship on regulating the data revolution (FL200100007) – see 'The Financial Data Revolution: Seizing the Benefits, Controlling the Risks' *fintechrevn* (Web Page, 2023) <https://fintechrevn.org/>. The views herein are of the authors and not necessarily of the Australian government or Research Council.

[1] See Statista Research Department, 'Leading Companies in the World in 2022*, by Pre-tax Income (In Billion U.S. Dollars)', *Statista* (Data Platform, 15 March 2023) <https://www.statista.com/statistics/269857/most-profitable-companies-

Oil has shaped our cities. It facilitated the post-war urban sprawl and connected cities by air and sea. But before oil, it was sanitation that made city living feasible. There is a photo of Manhattan from 1865 on our office wall. It shows Broad and Wall Streets with ten storey buildings and many horses and carts. Manhattan does not smell too good today in August – one can only wonder how it smelt with so many horses. Even so, densely populated Manhattan was habitable because clean water was piped in and sewerage was piped out, efficiently and safely.

Our consumer data-sharing regime will ensure businesses in the future have clean, reliable data to use, and can dispose of waste data safely. It will do for our data-driven economy what water and sewerage systems have long done for cities.

The metaphor – data is the new oil – may now underrate the power of data. Data is essential for the functioning of our information society. It is critical to everything from banking, healthcare and transportation to education, agriculture and real estate. Data enables better decision-making, increases efficiency, empowers businesses, and promotes social progress.

Just as water supply and sewerage disposal need to be well regulated to protect public health and promote economic development,[2] data needs to be well regulated so its value can be best realised. Historically, data was mostly controlled, and siloed, by the organisations that had the technological and financial resources to collect, store, and analyse it at scale. As a result, consumers often had little, if any, control over their data, and were unable to access or share it with others. A growing global awareness of these issues has prompted legislative data privacy frameworks like *the General Data Protection Regulation*[3] in the European Union ('EU') and the *California Consumer*

worldwide/#:~:text=In%202022%2C%20the%20Saudi%20Arabian,What%20is%20net%20income%3F>; see also 'Most Profitable Companies in the World for April 2023', *FinanceCharts* (Data Chart, 14 April 2023) <https://www.financecharts.com/screener/most-profitable>.

[2] See generally, Ramesha Chandrappa and Diganta B Das, *Sustainable Water Engineering: Theory and Practice* (Wiley, 2014).

[3] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1, which was adopted on 4 May 2016 and came into force on 25 May 2018.

Privacy Act (CCPA)[4] in the United States. Likewise, the Open Banking initiative in the United Kingdom ('UK') allows consumers to securely access and share their payment account data with third parties to access more tailored and innovative financial products and services.[5]

Nonetheless, Australia is currently the frontrunner among nations working on data-sharing regimes. The Consumer Data Right ('CDR') regime, introduced here in 2019, empowers consumers by giving them greater control over their personal data held by businesses; they can direct their data be transferred to other providers[6] who offer a better value for money service. The CDR regime returns data previously used by businesses for their own ends to consumers, who can now decide how it should be used for their benefit. Crucially, the regime is intended to span the economy. Initially rolled out in the banking sector, the CDR has been extended to the energy[7] and telecommunications[8] sectors, as well as to non-bank lenders.[9] However, most recently, to allow the CDR some time 'to mature' and also to ensure that the existing framework is functioning as effectively as possible, the Australian Government has made the decision to pause expansion into superannuation, insurance and telecommunications.[10]

---

[4] *California Consumer Privacy Act* §§1798.100-199 (2018) ('CCPA').

[5] Open Banking's origins lie in the banking sector in Europe. The revised *Payment Services Directive ('PSD2')* set the stage for account data retrieval and payment initiation by third parties in 2016. The UK was the first EU State to pass an Open Banking Standard to guide how financial data should be created, used, and shared by its custodians and those who access it. See *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/ EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC* [2015] OJ L 337/35 *('PSD2'*); Competition and Markets Authority (UK), *The Retail Banking Market Investigation Order 2017* (2 February 2017) pt 2, made under the *Enterprise Act 2002* (UK) and *Payment Services Regulation 2017* (UK) pt 7.

[6] See *Competition and Consumer Act 2010* (Cth) s 56AA ('*CCA*'), inserted by *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth) ('*CDR Act'*). Note, s 56AA(a)(i) of the *CCA* speaks of the right of consumers to request disclosure of their data to themselves, however, this right is not yet operative as no standards have yet been devised to implement it in practice; and furthermore, presumably most consumers lack access to the technology to safely access the data via the application programming interfaces ('APIs') through which that data is provided.

[7] *Consumer Data Right (Energy Sector) Designation 2020* (Cth).

[8] *Consumer Data Right (Telecommunications Sector) Designation 2022* (Cth).

[9] *Consumer Data Right (Non-Bank Lenders) Designation 2022* (Cth).

[10] Consumer Data Right, 'Consumer Data Right Newsletter: 26 May 2023' <https://mailchi.mp/f43e9452f613/consumer-data-right-newsletter-26-may-2023>.

This article analyses the idea of the CDR as a sanitation system for Australia's digital economy. We demonstrate how CDR offers a far more secure way to transfer consumer data than existing data-sharing arrangements. We also show how CDR's stringent accreditation process promotes the corporate 'consciousness-raising' that is needed to ensure that the legal obligations that apply to CDR participants (above all, data holders and accredited persons) are duly translated into practice.

Section 2 provides a brief overview of the CDR regime. Section 3 shows how standards, accreditation, consent and data integrity requirements provide for a robust system of pipelines delivering 'clean' data to consumers and businesses. Section 4 explains the 'hygiene' function built into the CDR ecosystem. Section 5 analyses the CDR in light of the privacy protections under the *Privacy Act 1988* (Cth) *('Privacy Act')* to show the added value of the CDR in protecting individuals' data. Section 6 concludes.

2. The CDR: Overview

The CDR is a robust infrastructure that enables an efficient and secure flow of data across the economy. It is grounded on the statutory framework of the *Treasury Laws (Consumer Data Right) Act 2019* (Cth) ('*CDR Act*')[11] which establishes stringent data quality control and transfer requirements and contains four core components. The first is the enabling legislation, the *CDR Act*. It introduces Part IVD into the *Competition and Consumer Act 2010* (Cth) ('*CCA*'),[12] which outlines the overarching objectives and principles of the CDR, sets out the role and functions of the regulatory bodies charged with establishing and enforcing CDR rules, and enshrines minimum privacy protections.[13] The second component is the CDR Designation Instruments issued under Part IVD of the *CDR Act,* which designate sectors of the Australian economy for the purposes of the CDR.[14] The CDR Rules are the third component of the framework and regulate the scope of

[11] *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth) ('*CDR Act*').

[12] *Competition and Consumer Act 2010* (Cth) ('*CCA'*).

[13] Australian Government, Treasury, *Consumer Data Right Overview* (Booklet, September 2019) 9 <https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf> ('CDR Booklet').

[14] For instance, the *Consumer Data Right (Authorised Deposit Taking Institutions) Designation 2019* (Cth) designated the banking sector.

data to be shared within a designated sector and the circumstances in which data sharing is required.[15] The Rules also set out privacy safeguards and regulate the use of data.[16] Finally, the fourth component – the Consumer Data Standards – stipulate the technical requirements by which data needs to be provided to consumers and accredited data recipients ('ADRs') within the CDR system (see also Subsection 3.1 below).[17]

The infrastructure is operated by multiple authorities. The rule-making responsibility lies with the Treasury: it has obligations to consult with the Australian Competition and Consumer Commission ('ACCC'), the Office of the Australian Information Commissioner ('OAIC'), the primary regulator of a given economy sector, and (when required by legislation) other stakeholders.[18] Enforcement of the CDR Rules and data standards is with the ACCC.[19] The Commission also accredits data recipients,[20] manages suspensions and revocations of accreditation[21] and maintains a register of accredited persons.[22] The OAIC enforces the privacy safeguards and privacy-related CDR rules and advises the Minister and CDR agencies on the privacy implications of the CDR Rules and data standards.[23] The data standards are made by the Data Standards Chair, assisted by the Data Standards Body.[24]

The principal entities that ensure the supply and transfer of 'potable' data as well as 'waste data' disposal are data holders, accredited persons and ADRs.[25] Data holders are those holding data

---

[15] *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) ('*CDR Rules*').

[16] Treasury, *Statutory Review of the Consumer Data Right* (Issues Paper, March 2022) 4.

[17] Ibid.

[18] *CCA* (n 11) ss 56BA(1), 56BQ, 56BP;; *Treasury Laws Amendment (2020 Measures No. 6) Act 2020* (Cth) sch 2 [34], [36].

[19] Ibid ss 56GD, 56FE(1)(a).

[20] Ibid ss 4, 56CA, 56CG.

[21] Ibid s 56CH; *CDR Rules* (n 14) r 5.17.

[22] Ibid s 56CE(1).

[23] Ibid ss 56EQ, 56ER, 56EU(3), 56EZ.

[24] Ibid ss 56FH, 56FK.

[25] The CDR also imposes obligations on 'designated gateways', i.e. entities designated by the Minister as responsible for facilitating the transfer of information between data holders and accredited persons: see *CCA* (n 11) s 56AL(2). See also Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) [1.72].

specified in a designation instrument.[26] Accredited persons are entities who have been 'licensed' by the ACCC to receive data through the CDR system.[27] Accredited persons who have collected CDR data from a data holder are referred to as ADRs.[28]

ADRs profit from accessing consumer data, as the data received improves their products and services and boosts their competitive position on the market. However, the ultimate beneficiaries of the regime are CDR consumers. Under the CDR, a consumer can be an individual or a legal entity.[29] The regime has no financial or other threshold test for non-individuals to be CDR consumers, meaning that businesses of all sizes can benefit from the CDR.[30]

The water in this digital system is 'CDR data' which covers information specified in a relevant instrument designating a sector and information subsequently wholly or partly derived from that data.[31] Designed to apply to 'key datasets', the regime has 'a strong focus on datasets that deliver tangible benefits for consumers either as a single dataset or in combination with others.'[32] There are generally two types of CDR data: data which identifies or makes a CDR consumer reasonably identifiable, and data about a product, good or service ('product data').[33] For example, in banking, data relating to a consumer includes customer data (ie information that identifies a consumer, such as individual or business name); account data (ie information that identifies the operation of the account, eg account number, balance, and authorisations); transaction data (eg the date of the

[26] *CCA* (n 11) s 56AJ(1).

[27] Ibid s 56CA.

[28] Note, however, that accredited persons can equally collect data from other ADRs: see *CCA* (n 11) s 56AK.

[29] See CCA (n 11) s 56AI (3), which speaks of 'persons' without further qualification; a 'person' can be either an individual or a legal entity. See also Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) [1.100].

[30] Maddocks, *Department of the Treasury: Consumer Data Right Regime* (Report, September 2019) 44 nn 34.

[31] *CCA* (n 11) s 56AI(1), 56AI(2).

[32] The Treasury, *Implementation of an Economy-Wide Consumer Data Right: Strategic Assessment, Consultation Paper* (July 2021) 8.

[33] *CCA* (n 11) ss 56AI, 56BE. Note that Privacy Safeguards discussed in Subsections 3.4-4.4 apply to CDR data 'for which there is a CDR consumer'.

transaction, amount credited or debited) and information that identifies or describes a certain product (eg type, name, pricing or features).[34]

In general terms, data qualifying as CDR data must be collected or generated *in* Australia. It can be 1) collected or generated by an Australian person, 2) relate to an Australian person, or 3) relate to goods or services offered to an Australian person.[35] If information is generated or collected *outside* Australia, it is covered only where the information is generated or collected by an Australian person *and* relates to an Australian person or goods and services supplied to an Australian person.[36] In practice, this means that if a CDR consumer uses her debit card issued by an Australian bank to make a purchase in Shanghai, then the transaction details must be available for the CDR consumer within the CDR regime.[37]

The CDR did not grow from nothing. Consumer data has long been shared between some businesses. For instance, credit providers have long had to provide certain information about credit accounts to credit reporting agencies (eg Equifax, Experian, and Illion) under the regime in Part IIIA of the *Privacy Act*. Banks have entered into bilateral agreements with certain data-driven service providers (eg accounting or budgeting software providers) to share data so as to provide additional functionality to their customers.[38] Data aggregators and businesses that offer financial technology solutions (FinTechs) have long accessed data through screen-scraping ('SS') technologies.[39] The objective of the CDR is to provide a framework that makes data sharing easier, more convenient and safer. As will be shown, CDR represents a step change in how customer data is handled and disclosed by businesses.

---

[34] See *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (Cth) ss 7, 8.

[35] *CCA* (n 11) s 56AC(3)(a).

[36] *CCA* (n 11) s 56AC(3)(b).

[37] See Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) [1.118].

[38] Australian Banking Association, *Code of Banking Practice* (at 5 October 2021).

[39] For further detail on the problem of SS, see below, Subsection 3.1. See also Natalia Jevglevskaja and Ross P Buckley 'Screen Scraping of Bank Customer Data: A Lamentable Practice' (2023) 23(3) *UNSW Law Research Paper*.

3. 'The Robust "Water" Supply System'

The CDR achieves efficient and secure flow of data by standardising how data is captured, stored, transmitted and protected, and by ensuring that only accredited entities partake in data collection, use and sharing. Through its standard setting and accreditation requirements, the CDR is thus granting a type of 'data safety licence' to CDR participants (Subsections 3.1 and 3.2).[40] Consumer consent – a fundamental aspect of the CDR ecosystem – serves as a 'valve' that allows, or stops, the flow of CDR data (Subsection 3.3). Finally, data integrity is built into the CDR to ensure that the data entering its ('water supply') system is 'clean' and 'potable' (Subsection 3.4).

3.1 Standards

Adequate treatment is essential for water to be safe to drink. Just as filters in a water supply system have standards for removing specific contaminants (be it bacteria, chemicals or sediment) to ensure the safety of the water, the CDR data standards – that is, information technology solutions that describe how CDR rules must be translated into practice – serve as filters that ensure data is treated in a consistent, secure manner. Where standards – as under the CDR – are consistent, technical and security updates can be applied more effectively, common problems solved more easily, and transaction costs for consumers using their data reduced.[41] Good standards are adaptable as they are responsive to changing demands for functionality. The drafters of the CDR therefore envisaged that these standards will be 'living documents',[42] and even where they may apply differently across sectors, interoperability would be achieved as far as practicable.[43]

There are many aspects to handling CDR data that require standardisation under the framework, including the format and description of CDR data; the collection, use, security and disclosure of CDR data; the process for obtaining and withdrawal of authorisations and consents; consumer

[40] Treasury, *Payments System Review* (Final Report, June 2021) 29; Treasury, *Future Directions: for the Consumer Data Right* (Final Report, October 2020) 192.

[41] Treasury, *Review into Open Banking: giving customers choice, convenience and confidence* (Final Report, December 2017) 188-189 ('*Review into Open Banking'*).

[42] Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) [1.266].

[43] Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) [1.265].

experience data standards, and many others.[44] Importantly, standards are enforceable. When a data standard applies, such as to a data holder or an accredited person, that standard operates as a contract between the data holder and accredited person; each party can enforce the contractual right under the CDR to access data in a format and manner consistent with the said standard.[45]

Through standardisation, the CDR fundamentally changes the way the data is transferred between businesses. It expedites and improves the exchange of information by standardising application programming interfaces ('API'). APIs enable software applications to communicate with each other over a network, using a common language and without intermediaries.[46] APIs tackle one of the key challenges to data portability: compatibility. To be portable, data needs to be stored in a commonly recognised format. Yet organisations have traditionally collected, stored and managed data (and often still do) in disparate ways, creating compatibility problems. APIs serve to translate one entity's data so that it can be understood by another. Standardisation of APIs enables work on a large scale and ensures safe, efficient and interoperable data-sharing architecture.[47]

The APIs of the CDR provide a far superior alternative to the lamentable screen scaping ('SS') practices still prevalent in banking and finance. In banking, SS involves gathering data by using a consumer's bank account login credentials. This access enables the scraping of data from the consumer's internet banking interface to offer her financial products and services.[48] SS allows businesses (mostly FinTechs) to see the customer data without their identification to the account hosting bank. It is now widely used globally, including in Australia, where reliance on SS has surged significantly in the past two decades.[49] It is hoped that the continuing rollout of the CDR will eventually end this practice in banking and finance.

---

[44] *CCA* (n 11) s 56FA(1). See also *CDR Rules* (n 14) r 8.11 and Part 8. For detailed information on these standards, see Data Standards Body, *Consumer Data Standards V1.23* (Electronic Standards) <www.consumerdatastandards.gov.au>.

[45] *CCA* (n 11) ss 56 FD, 56FE.

[46] On APIs generally, see Neil Madden, *API Security in Action* (Manning, November 2020) 6–8.

[47] See generally Krämer et al, *Making Data Portability More Effective for the Digital Economy: Economic Implications and Regulatory Challenges* (Centre on Regulation in Europe Report, June 2020).

[48] Jevglevskaja and Buckley (n 38); FinTech Australia, Submission No 182 to Productivity Commission, *Inquiry into Data Availability and Use: Open Financial Dat*a (August 2016) 4.

[49] Australian Securities and Investments Commission, 'Account Aggregation in the Financial Services Sector' (Consultation Paper No 20, May 2001) 19. See also *Review into Open Banking* (n 40) 51. In 2020 the Senate Select

The scope, consistency and enforceability of CDR standards sets the CDR apart from other legal frameworks that regulate data-portability,[50] such as the EU General Data Protection Regulation ('GDPR'). Article 20 GDPR provides data subjects with the right to receive their personal data in a 'structured, commonly used, and machine-readable format' and to transfer that data to another controller without hindrance. To facilitate this right, the European Data Protection Board ('EDPB') has issued guidelines on how to interpret and implement the right to data portability.[51] While these guidelines strongly encourage cooperation between industry stakeholders and trade associations in working together 'on a common set of interoperable standards and formats to deliver the requirements of the right to data portability',[52] the pivotal supportive infrastructure around Article 20 GDPR that enables the law to efficiently operate in practice remains (due to the nature of the European Union) fragmented. Above all, Europe has no mechanism similar to that under the CDR to impose and enforce a consistent set of standards in any given economic sector, let alone economy-wide. To illustrate, the sharing of payment account data in the European banking industry has been significantly spurred by the revised Payment Services Directive (PSD2)[53], with three main API standards co-existing: the STET PSD2 API framework, UK Open Banking Standard, and Berlin Group's NextGenPSD2 XS2A Framework Standard. Each of the standards come with different specifications or requirements for its region, which are then often further particularised by individual banks.[54]

Committee on Financial Technology and Regulatory Technology confirmed that the technology was still *widely used* by banks, lenders, financial management applications, personal finance dashboards, and accounting products: Senate Select Committee on Financial Technology and Regulatory Technology, Parliament of Australia, *Interim Report* (Report, September 2020) [5.50].

[50] Note that the scope of the UK's Open Banking initiative with its detailed set of standards and guidelines is focused on sharing payment account data and is thus much more limited than the scope of the CDR (see above, Section 1).

[51] European Data Protection Board, *Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01* (Guidelines, 5 April 2017) <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-right-data-portability-under-regulation-2016679_en>.

[52] Ibid 18.

[53] Ibid s 1 nn 3.

[54] Ibid. See also Andrei Cazacu, 'PSD2: Does Europe Need a Single API Standard?', *TrueLayer* (Blog Post, 13 July 2022) <https://truelayer.com/blog/psd2-does-europe-need-a-single-api/>.

3.2 Accreditation

To ensure that 'the water' in this digital ecosystem is supplied by and transferred between providers that are trusted, the CDR establishes stringent accreditation requirements. To have CDR data disclosed to them, businesses must be accredited. An accredited person must fulfill a set of conditions: 1) be a fit and proper person or organisation;[55] 2) have processes in place to adequately protect data;[56] 3) have internal dispute resolution processes;[57] 4) belong to a relevant external dispute resolution scheme;[58] 5) hold adequate insurance due to the risk of CDR consumers not being properly compensated for losses that might reasonably be expected to arise from a breach of obligations under the CDR framework;[59] 6) and have an Australian address for service.[60]

Two levels of accreditation are available to CDR participants: the unrestricted level, which is the highest level, and the sponsored level, which imposes certain limitations on participation in the CDR system of the 'sponsored' participant. Unrestricted level participants can collect CDR data from data holders with the consumer's consent. In addition to meeting the above stated accreditation criteria, unrestricted participants must submit an independent third-party assurance report as part of their accreditation application. This provides an assessment in accordance with the Standard on Assurance Engagements (ASAE 3150)[61] on whether the said participant's systems and processes meet the requisite CDR information security requirements.[62] In contrast, sponsored participants – known as 'affiliates' – while subject to the same accreditation criteria as unrestricted participants, do not have to provide an independent third-party assurance report. They instead use the sponsored accreditation self-assessment and attestation form to self-assess and attest to their

[55] *CDR Rules* (n 14) rr 1.9, 5.12 (2)(a).

[56] Ibid r 5.12(1)(a).

[57] Ibid r 5.12(1)(b).

[58] Ibid r 5.12(1)(c).

[59] Ibid r 5.12(2)(b).

[60] Ibid rr 1.7 (definition of 'addresses for service'), 5.12(d), 5.12(e).

[61] See Auditing and Assurance Standards Board, *Standard on Assurance Engagements: Assurance Engagements on Controls* (ASAE 3150, January 2015) and *CDR Rules* (n 14) r 2.1(1)(a)(i).

[62] *CDR Rules* (n 14) r 2.1(1). See also Australian Government, *Accreditation Fact Sheet* (Fact Sheet Version 2, December 2022) 3 <https://www.cdr.gov.au/sites/default/files/2022-12/CDR-Accreditation-fact-sheet-version-2-December-2022.pdf>.

ability to meet the requisite information security requirements.[63] Affiliates cannot collect CDR directly from a data holder, only from ADRs[64] or their sponsors who collect CDR data from CDR participants on the affiliates' behalf.[65] An affiliate must also have a sponsorship arrangement with a sponsor, whereby the sponsor agrees to disclose to the affiliate CDR data it holds as an ADR, and the affiliate undertakes to provide the sponsor with such information and access to its operations as is needed for the sponsor to comply with its sponsorship obligations.[66] Like all ADRs, affiliates are generally responsible for their use and disclosure of CDR data they receive.[67]

By requiring all applicants to meet the same minimum obligations for handling and protecting consumer data, the CDR accreditation requirements create a level-playing field among participating businesses and helps consumers trust these providers with their data. A failure to do so risks rejection of the application, as experienced most recently by iSignthis Australia Pty Ltd ('iSignthis'). The ACCC refused to accredit iSignthis following significant doubts as to whether it was a fit and proper person under the CDR regime, and whether it could comply with the ADR's duties.[68]

Making the case for compliance – that is, demonstrating that the applicant has the necessary technical, security, and governance systems in place to comply with the CDR legislative and regulatory requirements – assists organisations in identifying where improvements or adjustments should be made to their systems and processes to better handle consumer data responsibly. At a minimum, accreditation thus serves as a corporate 'awareness' or 'consciousness' raising exercise about the obligations under the CDR regime (in particular, the risks associated with handling

[63] Fact Sheet (n 62).

[64] Via a consumer data request: *CDR Rules* (n 14) r 4.7A.

[65] *CDR Rules* (n 14) r 5.1B(3).

[66] Ibid r 1.10D.

[67] The sponsor and affiliate may agree, however, that the sponsor may make CDR requests, or use or disclose CDR data, at the request of the affiliate. In this case, the sponsor would be acting on its own behalf, and be liable for its actions, when it makes consumer data requests, uses or discloses the data. See Minister for Superannuation, Financial Services and the Digital Economy (Cth), *Exposure Draft Explanatory Materials: (Consumer Data Right) Amendment (2021 Measures No. 1) Rules 2021* (1 July 2021) 6-7.

[68] Australian Competition and Consumer Commission, 'iSignthis refused Consumer Data Right accreditation', *ACCC* (Media Release, 15 December 2022) <https://www.accc.gov.au/media-release/isignthis-refused-consumer-data-right-accreditation>.

consumer data and the measures required to protect it) and the potential consequences of non-compliance.

Indeed, the CDR's enforcement and remedy regime – applied through obligations and penalty provisions contained in both the *CCA* and the CDR Rules[69] – provides a strong compliance incentive for accredited entities. Above all (as will be shown in detail below), all but one of the Privacy Safeguards – the legally binding statutory provisions that ensure the security and integrity of the CDR system[70] – are civil penalty provisions. The high penalties reflect the value ascribed to consumer data. Maximum penalties for entities (ie body corporates) could be, for example, the greater of AUD $10,000,000 or, if the court can determine the value of the benefit 'reasonably attributable' to the act or omission, three times that value.[71] For entities that are not body corporates, the maximum amount of AUD $500,000 applies.[72] Moreover, the failure to comply with the CDR may not only lead to significant reputational damage but also to suspension or revocation of accreditation.[73]

The recent large-scale attack on Optus – which some experts suggest may be the worst data breach in Australia's history[74] – illustrates vividly how accreditation under the CDR can help prevent unforgivable mishandling of consumer data. The security breach resulted in the unauthorised disclosure of personal information of up to 9.8 million Optus customers – about 40% of Australia's population – and included 'customers' names, dates of birth, phone numbers, email addresses, addresses and ID document numbers such as driver's licence or passport numbers, exposing

[69] *CCA* (n 11) ss 56BO(1), 56BU(1), 56CD; *CDR Rules* (n 14) r 9.8.

[70] OAIC, *Consumer Data Right: Privacy Safeguard Guidelines* (Guidelines Version 4.0, November 2022) para A.10 <https://www.oaic.gov.au/__data/assets/pdf_file/0013/24034/Privacy-Safeguard-Guidelines-v4-Nov-2022-rev2.pdf>.

[71] Note: if the Court cannot determine the value of that benefit, a penalty of up to 10% of the body corporate's adjusted turnover during the 12-month period ending at the end of the month in which the act or omission occurred or started to occur applies: see *CCA* (n 11) s 76(1C)(c).

[72] *CCA* (n 11) ss 76(1)(a)(ib), 76(1)(a)(ib)(1A).

[73] See, for example, *CCA* (n 11) ss 56EA, 56BH(3).

[74] Tiffanie Turnbull, 'Optus: How a Massive Data Breach Has Exposed Australia', *BBC News* (online, 29 September 2022) <https://www.bbc.com/news/world-australia-63056838>.

affected consumers to a significant risk of identity theft and fraud.[75] Notably, the identity documents of some 900,000 customers had expired, and for all customers, once their identity had been verified, retaining the data of such documents was a highly questionable practice.[76] It is also reported that Optus's API did not require authorisation or authentication to access customer data, meaning that anyone on the internet with knowledge of that API endpoint could use it.[77] Had Optus been accredited under the CDR, it would likely have been in violation of its CDR obligations (discussed in more detail in Sections 4.1 and 4.3 below) by holding on to out of date data, and certainly for failing to protect its customer data from unauthorised access – and potential subsequent misuse – by breaching the minimum information security controls. Still, in the first place, the probability of violations occurring at such scale would have been significantly diminished by the corporate consciousness-raising exercise the stringent CDR accreditation process invariably triggers.

Although accreditation is of utmost significance in getting closer to valuable consumer data, it is but the first step in that process. The valve that opens the flow of data in the direction of accredited persons is consumer consent, and is the focus of the next subsection. While the legislative and regulatory requirements analysed in the remainder of Sections 3 and 4 extend (depending on the context) to a range of CDR participants discussed in Subsection 2.2 above, reference, for the purposes of our argument, will be limited to data holders, accredited persons, and ADRs.

3.3 Consent

The 'water' supply in the CDR data ecosystem is squarely dependent on consumer consent, touted as 'the bedrock' of the CDR.[78] Data holders must ask consumers to authorise disclosure of

[75] 'Optus Notifies Customers of Cyberattack Compromising Customer Information', *Optus* (Media Release, 22 September 2022) <https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack>.

[76] 'Optus CEO Kelly Bayer Rosmarin's Video Statement About Data Leak', *7NEWS* (online, October 2022) <https://www.youtube.com/watch?v=0tSUdfriozU>.

[77] Josh Taylor, 'Optus Data Breach: Everything We Know So Far About What Happened', *The Guardian* (online, 29 September 2022) <https://www.theguardian.com/business/2022/sep/29/optus-data-breach-everything-we-know-so-far-about-what-happened>.

[78] OAIC (n 70) para C2.

requested CDR data and keep records and explanations of authorisations provided by consumers.[79] ADRs must also have consumer consent to request consumer data. Consent cannot be 'implied' or 'open ended'; consumers must understand what they are consenting to and be able to revoke their consent to data disclosure, collection or use at any time.[80]

The increased strength that consent requirements bring to the CDR is best illustrated by comparison with the consent requirements stipulated in the *Privacy Act*. Set up to promote and protect the privacy of individuals and to ensure that the privacy protections are duly balanced with the interests of organisations that handle individuals' data, the privacy framework has been governing data *collection* and *use* in Australia for over thirty-five years.[81] The cornerstone of the privacy protection framework under the *Privacy Act* are the thirteen Australian Privacy Principles ('APPs'), which prescribe standards, rights and obligations in relation to handling, holding, accessing and correcting personal information. Importantly, the CDR Privacy Safeguards ('PSs') that protect the privacy or confidentiality of consumer data under the CDR (and discussed in more detail in the remainder of this paper) are modelled on the existing APPs, albeit with additional obligations.[82]

Consent is relevant to the operation of several APPs and PSs. First, where data collection under the CDR occurs without the requisite consumer permission, the data must be destroyed as soon as practicable.[83] Conversely, under the *Privacy Act*, APP entities (that are 'organisations'[84]) can collect personal information (other than sensitive information) if the information 'is reasonably

[79] *CCA* (n 11) s 56BC(2); *CDR Rules* (n 14) rr 4.5(2), 9.3(1).

[80] *CCA* (n 11) s 56BC(2); *CDR Rules* (n 14) rr 4.8-4.9, 4.11-4.12.

[81] *Privacy Act 1988* (Cth) s 2A ('Privacy Act')

[82] As mentioned previously, PSs apply to CDR data for which there is a CDR consumer. Further, PS apply mainly to accredited persons and designated gateways, in relation to their handling or future handling of the CDR data: *CCA* (n 11) s 56EA. The *Privacy Act 1988* and the APPs continue to apply to data holders under the CDR with the exception of APPs 10 and 13 which are replaced by PSs 11 and 13 once the data holder is required or authorised to disclose the CDR data under the CDR Rules. PS 10 does not have an APP equivalent and applies to data holders in addition to all other privacy protections. PS 1 applies to data holders in parallel to APP 1. See also OAIC (n 70) para C2.

[83] *CCA* (n 11) s 56EF. The destruction requirement applies unless an accredited person is required to retain that CDR data by or under an Australian law or a court/tribunal order': at s 56EG. See also Subsection 4.4 below.

[84] Note that an 'APP entity' can be either an 'agency' or 'organisation', defined respectively in *Privacy Act* (n 81) ss 6(1), 6C.

necessary for one or more of the entity's functions or activities'.[85] Restated, personal data can be collected without consent under the privacy framework provided it is not sensitive information.[86] Second, where consent is required because the information is 'sensitive', consent may be 'implied' under the *Privacy Act* upon making a reasonably inference in the circumstances from the individual's conduct.[87] Under the CDR, 'implied' consent may never serve to underpin data collection or disclosure.[88]

Third, under the CDR, data must only be used for the purpose for which the consumer has given her consent.[89] By comparison, the *Privacy Act* permits the use of personal data for purposes other than the primary purpose of collection, provided the individual could reasonably expect the entity to use her data for the secondary purpose and that purpose is related to the primary purpose of collection.[90] Where, for example, an individual openly criticises an APP entity about the way it treated her personal information, the *Privacy Act* presumes that she may reasonably expect that the entity may respond to these criticisms publicly and thereby reveal personal data related to the issues she raised.[91]

Fourth, under the CDR regime, ADRs must not use or disclose CDR data for the purposes of direct marketing unless explicitly requested to do so by the consumer.[92] Direct marketing involves the use or disclosure of consumer data to communicate directly with individual consumers via direct channels like email or telephone to promote goods and services (rather than advertising for a mass

---

[85] *Privacy Act* (n 81) s 3.1-3.2.

[86] 'Sensitive information' is defined in the *Privacy Act 1988* (Cth) s 6(1). On the range of data covered under the CDR and *Privacy Act*, see below, Section 5.

[87] *Privacy Act* (n 81) s 6(1); OAIC, *Australian Privacy Principles Guidelines* (Guidelines Version 1.2, combined December 2022) para B.40.

[88] See *CDR Rules* (n 14) r 4.9 explicitly listing the requirements for consent to be 'express' and 'specific as to purpose'.

[89] *CCA* (n 11) s 56EI(1)(a); *CDR Rules* (n 14) r 4.9, explicitly listing the requirements for consent to be 'express' and 'specific as to purpose'.

[90] Or is 'directly related' to the primary purpose if the information is 'sensitive information': see *Privacy Act* (n 81) sch 1, s 6(2).

[91] See *L v Commonwealth Agency* [2010] PrivCmrA 14 (24 December 2010); see also OAIC (n 87) para 6.22.

[92] *CCA* (n 11) s 56EJ.

audience, typically through broadcast media).[93] Contrast the CDR approach with the broader permissions under the *Privacy Act*: an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if the individual could reasonably expect it to do so and the organisation is otherwise compliant with the *Privacy Act*.[94]

These few comparisons illustrate that a consumer has considerably greater control over the access and management of her data under the CDR framework than the privacy framework. Consumers have the power to drive the flow of data in the direction that promises the most value from it, and can be confident that unless they have specifically requested to be contacted by businesses that directly market their products and services, the water in the system will not be turned against them and flood them with unsolicited phone calls or emails.

3.4 Data Quality

Just as water can be polluted by contaminants, data can be 'non-potable', or unreliable, because of errors, inaccuracies or biases or from becoming outdated or manipulated. To ensure integrity and reliability of data, the CDR sets out a rigorous set of rules on data collection, use, storage, deletion, correction, and disclosure. In particular, PS 11 mandates that if a data holder or an ADR are required or authorised under the CDR rules to disclose the CDR data they hold, they must take reasonable steps to ensure that it is 'accurate, up to date and complete' for the 'purpose for which it is held.'[95] While neither of these terms are defined under the *CCA* or the CDR rules, the OAIC reads the requirement to mean that the consumer data must contain no errors, defects or be misleading; be current at, or throughout, the time the data holder is required or authorised to disclose the CDR data (or in the case of an ADR, at the time of disclosure); and present the full (rather than partial) picture of the matter.[96] The wording further suggests that the requirement is

[93] See OAIC (n 87) 3, ch 7.

[94] That is, the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation and the individual has not made such a request to the organisation: see *Privacy Act* (n 81) sch 1, s 7(2).

[95] See *CCA* (n 11) ss 56EN(1), 56EN(2); see also *CDR Rules* (n 14) rr 7.10-7.10A.

[96] OAIC (n 70) paras 11.22, 11.26, 11.29; Derived data would be inaccurate, for example, where the basis for its analysis is wrong or inappropriate: at paras 11.23-11.24.

cumulative: compliance with one of the requirements does not suggest that other requirements are equally likely to be satisfied. Where, for example, the consumer has changed her employer (for instance, moved from one university to another) but her CDR data shows that she is still working for the former institution, the data could legitimately be regarded as 'up to date' if it is held for the purpose of recording whether the consumer is an academic. It will be inaccurate and incomplete, however, if it is held for the purpose of recording eligibility for certain academic benefits, such as long service leave, if the new institution does not recognise prior service elsewhere.

Designed to ensure consumer confidence in the quality of their CDR data,[97] PS 11 also mandates that a data holder or an ADR who has disclosed incorrect CDR data to an accredited person must inform the affected consumer and, should that consumer request rectification of the mistake, disclose corrected CDR data to the original recipient.[98] The record keeping requirements apply: the data holder must maintain the record of both the initial and the subsequent disclosures; the ADR must also record both the initial collection of the incorrect CDR data and the subsequent collection of the corrected CDR data.[99]

4. 'The Hygiene Function'

On top of building a robust 'water supply system', the CDR also performs an important hygiene function to ensure that the properties of data required under PS 11 – accuracy, currency and completeness – are maintained. This function is reflected in the obligations to:

- adequately protect, or preserve the integrity of, 'accurate, up to date and complete' CDR data (Subsection 4.1);
- correct CDR data where necessary (Subsection 4.2);
- delete or de-identify 'redundant' CDR data (Subsection 4.3); and
- destroy unsolicited CDR data (Subsection 4.4).

This section addresses each of these obligations in turn.

[97] OAIC (n 70) para 11.6.

[98] *CCA* (n 11) ss 56EN(3), 56EN(4).

[99] *CDR Rules* (n 14) rr 9.3(1)(d), 9.3(2)(e).

4.1 Protection of CDR Data

Faster and more efficient data access, particularly by third parties, risks exacerbating existing privacy risks and introducing new ones. Inadequate information security practices may expose the systems, services and data they host to cyber-attacks. This affects both individuals whose data integrity is compromised and the data-hosting businesses missing out on potential commercial opportunities after losing clients due to the security breach. Against this background, PS 12 imposes strict and detailed information security requirements,[100] including an extensive set of minimum information security controls[101] that an ADR should implement to protect CDR data from 'misuse, interference and loss' and 'unauthorised access, modification or disclosure'.[102] Information security in the context of PS 12 covers both cybersecurity (ie integrity of networks and information systems) and physical and organisational security measures.[103]

Broadly, the steps that must be taken by ADRs to manage the information security of CDR data effectively include:

1) defining and implementing security governance in relation to CDR data; this governance framework should be informed by the analysis of the ADR's information security risk posture (ie the exposure and potential harm to its information assets, including CDR data, from security threats) and contain practices, procedures and information security controls established to mitigate those risks[104]

2) defining the boundaries of the CDR data environment; this includes identifying the people, processes and technology that an ADR relies on to manage the CDR data infrastructure to ensure that the ADR is fully aware of what CDR data it has, who has access to it and what kind of risks to the safety and security of that data exist[105]

---

[100] Ibid sch 2, Part 1.

[101] Ibid sch 2, Part 2.

[102] See *CCA* (n 11) s 56EO(1); *CDR Rules* (n 14) sch 2. While the terms 'misuse, interference and loss' and 'unauthorised access, modification or disclosure' are not authoritatively defined under the CDR framework, the OAIC has offered some interpretative guidance based on the ordinary meaning of these terms: OAIC (n 70) para 12.18.

[103] *CDR Rules* (n 14) sch 2, s 1.2.

[104] Ibid sch 2, s 1.3.

[105] Ibid sch 2, s 1.4.

3) establishing and maintaining an information security capability; this ensures compliance with the minimum security controls detailed in the CDR Rules[106]
4) implementing a formal controls assessment program by establishing a testing program to review and assess the effectiveness of the ADR's information security capability; this testing program should be reviewed for its sufficiency at least annually or following any material change to the nature and extent of threats to the ADR's CDR data environment,[107] and
5) managing security incidents, covering all stages from detection to post-incident review, and reporting security breaches to the Information Commissioner, CDR consumers[108], and the Australian Cyber Security Centre within the Australian Signals Directorate.[109]

PS 12 and accompanying CDR Rules thus seek to ensure that compliance with information security requirements is not simply an afterthought or a mere 'box-ticking' exercise that can be treated in isolation from broader organisational frameworks.[110] Rather, it mandates that information security measures are properly integrated into an ADR's overall risk management strategy and – through its detailed specifications in the CDR Rules – guides businesses in implementing a consistent, robust standard of data security. This requirement is complemented by the obligation to correct CDR data in response to a consumer request which we discuss next.

4.2 Correction of CDR Data

For consumers to fully benefit from the CDR system by receiving better-quality offers from other service providers, they need assurance that the data disclosed to those providers is reliable. Given that data may easily become inaccurate or quickly lose its currency if not appropriately managed or maintained, PS 13 mandates that data holders and ADRs react to the consumer request to correct

[106] Ibid sch 2, s 1.5, pt 2.

[107] Ibid sch 2, s 1.6.

[108] As required under the *Privacy Act* (n 81) pt IIIC. Note that the Notifiable Data Breaches (NDB) provisions in Part IIIC of the *Privacy Act* apply to ADRs as if personal information in the sense of NDB provisions were 'CDR data': *CCA* (n 11) s 56ES(1).

[109] *CDR Rules* (n 14) sch 2, s 1.7.

[110] OAIC (n 70) 10, ch 12.

her CDR data by either correcting it or issuing a qualifying statement that the CDR data – in view of the purpose for which it is held – is accurate, up to date, complete and not misleading.[111]

By giving the consumer a tool to instigate correction of her CDR data to prevent any negative outcomes that could arise from the sharing of inaccurate information, PS 13 supplements PS 11 (discussed in Subsection 3.4 above) which imposes an obligation on data holders and ADRs to ensure that the CDR data is free of errors, current and sufficient.[112] Reasons for not correcting CDR data or including a qualifying statement with the data may be, for example, that the consumer is mistaken and has made the correction request in error, or that despite some inaccuracies in the data, it is nevertheless accurate, up to date, complete and not misleading for the purpose for which it is held. For instance, where a consumer has purchased a second or third car but her CDR data records her as only possessing one vehicle, no correction would be needed if the data is held for the purpose of recording whether the consumer is a driver.[113] To ensure that any qualifying statement is prominently displayed to those who access the data, data holders and ADRs must, where practicable, provide an electronic link to a digital record of that data.[114]

PS 13 places equal emphasis on mandating transparency and ensuring that correction requests are responded to promptly. Regardless of the course of action taken in a given case, the consumer must be appropriately notified by electronic means.[115] The notice must set out whether: 1) the data has been corrected or not; 2) if no action was taken, why a correction or qualifying statement was unnecessary; and 3) specify complaint mechanisms available to the consumer.[116] The notice must be served to the consumer within ten business days of the request being filed.[117] Under the *Privacy Act*, the APP entity can operate under comparatively extended deadlines: if the entity is an agency,

[111] See *CCA* (n 11) s 56EP.

[112] OAIC (n 70) para 13.9.

[113] Ibid para 13.30.

[114] *CDR Rules* (n 14) r 7.15(b).

[115] See *CCA* (n 11) ss 56EP(3)(b); *CDR Rules* (n 14) r 7.15(c).

[116] *CDR Rules* (n 14) r 7.15(c).

[117] Ibid r 7.15(b).

the response is due within 30 days after the request is made, and if the entity is an organisation, within a reasonable period.[118]

Where a data holder or an ADR corrects CDR data, it should determine what to do with the original data. The following subsection discusses options available under the CDR framework.

4.3 Deletion and De-identification of CDR Data

Where an ADR no longer needs the CDR data for purposes permitted under the PSs or the CDR Rules, the data is considered 'redundant data' and, unless an exception applies, must be destroyed or de-identified.[119] CDR data becomes automatically redundant with the expiry of the consumer permission to use it and where an ADR's accreditation is surrendered or revoked.[120] Exceptions to the destruction or de-identification requirement include where the ADR is required to retain the redundant data by an Australian law, court or tribunal; or where the redundant data relates to any current or anticipated legal or dispute resolution proceedings to which the ADR is a party.[121]

Whether data must be deleted or de-identified depends on a range of factors. An ADR may have a general policy of deleting redundant data.[122] Where, after initially requesting consumer consent to handle CDR data, the ADR has advised the consumer of a general policy of destruction, the ADR must destroy the redundant data even if its general policy has since been revised.[123]

ADRs may also have a general policy of de-identifying redundant data or deciding whether to delete or de-identify the CDR data when it becomes redundant.[124] In either case, however, the ADR must allow the consumer to elect for her redundant data to be deleted at the time of requesting

---

[118] *Privacy Act* (n 81) sch 1, ss 13.5, and definitions in ss 6(1) , 6C.

[119] *CCA* (n 11) ss 56EO(2), 56BAA(1); *CDR Rules* (n 14) rr 1.17-1.18, 7.11-7.13.

[120] *CDR Rules* (n 14) r 5.23(4)(a). Likewise, where a consumer has several accounts with a data holder, and data associated with one of those accounts is no longer needed by the ADR for the provision of the requested services, that account data becomes 'redundant' in the sense of the *CDR Rules*: see OAIC (n 70) para 12.90.

[121] *CCA* (n 11) ss 56EO(2)(b), 56EO(2)(c).

[122] *CDR Rules* (n 14) r 4.17(1)(a).

[123] OAIC (n 70) para 12.97.

[124] *CDR Rules* (n 14) rr 4.17(1)(b), 4.17(1)(c).

consumer consent and at any time thereafter.[125] To the extent that the consumer is identifiable or reasonably identifiable from the derived data, the deletion request covers any data derived from her CDR data.[126]

Where de-identification is technically feasible and the ADR wants to pursue this option, it must ensure that the data is de-identified to the extent mandated under the CDR framework.[127] The conditions imposed on the de-identification process are stringent. In particular, the ADR must consider the suitability of the CDR data for release into the public environment (regardless of whether the data will in fact be released). Restated, the ADR must consider the possibility of re-identification of a CDR consumer by any third party on the basis of the de-identified data and any other information on that CDR consumer that the third party may possess.[128] De-identification is only permitted where there is 'a very high degree of confidence, that no persons are reasonably identifiable.'[129] If such a level of confidence cannot be achieved, the CDR data and any data derived from it must be deleted in accordance with the CDR Rules.[130]

In view of the consumer prerogative to withdraw her consent to data collection, use or disclosure at any time[131] or limit the time in which a data recipient can hold her CDR data,[132] the regime would be incomplete without the corollary obligation on ADRs to delete or de-identify redundant CDR data. Notably, the right of a consumer to *instruct deletion of her CDR data* (where, as explained previously, an ADR has a general policy of de-identification of the CDR data) is one of unique aspects of the CDR.[133] No such right currently exists under the *Privacy Act*. The requirement 'to take reasonable steps' to destroy or de-identify personal information set out in

[125] Ibid r 4.16(1).

[126] Ibid r 4.16(1).

[127] *CDR Rules* (n 14) rr 1.17(2), 7.12(2).

[128] Ibid r 1.17(2). Further guidance is provided in Christine O'Keefe et al, *The De-Identification Decision-Making Framework* (CSIRO Report EP173122, 18 September 2017).

[129] OAIC (n 70) para 12.105.

[130] *CDR Rules* (n 14) r 1.17(4).

[131] Ibid r 4.13(1).

[132] Ibid r 4.11(1)(b).

[133] See also *Review into Open Banking* (n 40) 57.

APP 11 is articulated as a duty imposed on an APP entity and has no corresponding entitlement to request such deletion by the consumer.[134]

In its commitment to transparency, the CDR mandates that where data is deleted, a record to evidence the deletion must be made.[135] In case of data de-identification, the requirements are considerably more detailed as an ADR must record: 1) the details of the assessment so that it is possible to de-identify the relevant data to the extent required under the CDR rules; 2) that the relevant data was de-identified to that extent; 3) how the relevant data was de-identified, including records of the technique that was used; and 4) any persons to whom the de-identified data has been disclosed.[136]

4.4 Destruction of Unsolicited CDR Data

Accredited persons may find themselves in possession of CDR data they had not sought after requesting particular CDR data from a data holder. For example, a data holder may disclose CDR data that includes data outside the scope of the consumer data request. In such a case, accredited persons must destroy the unsolicited data as soon as practicable unless required by Australian law to retain it.[137] Destruction of CDR data should follow the CDR data deletion process. This PS 4 aims to enhance the protection provided to CDR consumers by limiting the amount of data that businesses can retain to only what has been authorised by the consumer, thereby also reducing the risk of data breach.[138]

Unlike the CDR regime, individuals have far less insight into when their 'unsolicited' data may be destroyed under the *Privacy Act*. Under APP 4, 'unsolicited data' may be retained even where retention is not mandated by law or a court or tribunal order, provided the data could have been

[134] Australian Government, Attorney General's Department, *Privacy Act Review* (Report 2022, 16 February 2023) 166 <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf> ('*Privacy Act Review'*).

[135] *CDR Rules* (n 14) r 1.18.

[136] Ibid r 1.17(3)(d).

[137] *CCA* (n 11) s 56 EG.

[138] OAIC (n 70) paras 4.4-5, 12.127.

collected under the privacy principle regulating collection of solicited data.[139] As mentioned earlier (Subsection 3.3), collection of personal information (other than sensitive information) by APP entities (ie organisations) is permitted if the information 'is reasonably necessary for one or more of the entity's functions or activities'.[140] But even where the APP entity determines that the entity should not have collected the personal information,[141] the destruction or de-identification requirement applies only if destruction is both 'lawful' and 'reasonable'.[142] What is 'reasonably necessary' or 'reasonable' depends on the circumstances of each individual case and while an objective standard applies – a standard that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances[143] – the inherent elasticity of the concept gives APP entities the prerogative to retain data they may not be able to keep under the CDR.

5. The Added Value of CDR's Privacy Safeguards

Our analysis highlights how the CDR's consent requirements and privacy protections go beyond those of the APPs that continue to operate alongside the CDR in relation to personal information (that is not CDR data) held by APP entities.[144] It shows how the CDR's consent requirements enable consumers to be the true decision makers in the ecosystem and exposes numerous shortcomings of the APPs in adequately protecting individuals' data. The analogy of the CDR with a well-functioning water supply and sanitation system would be incomplete, however, without a more holistic consideration of the strengths of the CDR framework that the APPs have long been unable to claim.

As seen, the differences between the PSs and the APPs are many and some are substantial. In a nutshell, the CDR imposes obligations on a broader range of entities, covers larger sets of data, and applies equally stringent protections to all designated data it covers. Crucially, the CDR can better respond to evolving privacy risks and provides for a much stronger enforcement mechanism

[139] *Privacy Act* (n 81) sch 1, s 4.

[140] Ibid sch 1, ss 3.1, 3.2.

[141] and the information is not contained in a Commonwealth record (in the sense of the *Archives Act 1983* (Cth) s 6(1)).

[142] *Privacy Act* (n 81) sch 1, s 4.3.

[143] OAIC (n 87) para 4.24.

[144] See also n 82, explaining how APPs apply to data holders under the CDR.

where the APPs remain a 'toothless tiger'. These stronger protections under the CDR have been put in place to mitigate risks associated with faster and more convenient transfers of CDR data. We now illustrate each of these points.

First, PSs impose obligations on businesses not covered by the *Privacy Act*. APPs generally apply to Australian Government agencies and organisations with an annual turnover exceeding $3 million. Small businesses with a turnover of $3 million or less are excluded from the *Privacy Act*[145] unless, for example, they sell or purchase personal information or are data holders under the CDR regime.[146] In contrast, PSs are contingent on accreditation and apply to data holders, accredited persons and ADRs regardless of the size of the business.

Second, PSs have a more extensive data coverage. As mentioned previously, CDR applies to 'CDR data' as specified in a given designation instrument. Broadly, two types of data are covered: first, data about a product, good or service which does not identify any individual CDR consumer; and second, data that *relates to a person*[147] or, using the legislative language, data 'for which there are one or more CDR consumers'.[148] PSs apply to the second types of data meaning that there needs to be at least one person who is identifiable, or reasonably identifiable, from the CDR data.[149] Notably, and unlike the APPs, the PSs apply to CDR data where the CDR consumer is a *business*. In contrast, the APPs leave business information outside of their protective scope: they apply to 'personal information', which is defined to include information or an opinion *about* an 'individual' (ie natural person) from which the individual can be identified.[150]

---

[145] *Privacy Act* (n 81) s 6C(1).

[146] *Privacy Act* (n 81) ss 6D (4)(c), (4)(d). For other small business operators covered by the *Privacy Act*, see at s 6D (4). See also 'Rights and Responsibilities' *OAIC* (Web Page) <https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/rights-and-responsibilities#WhoHasResponsibilitiesUnderPrivacyAct>.

[147] See *CCA* (n 11) s 56AI (3)(a) (emphasis added).

[148] Ibid s 56EB(1).

[149] Or from related information held, for example, by a data holder or an ADR: see *CCA* (n 11) s 56AI(3)(c).

[150] *Privacy Act* (n 81) ss 2A(c), 2A(d), s 6(1) (emphasis added).

In contrast to data *about* an individual protected by the APPs, the use of the term 'relates' establishes a lower threshold for information to be protected by the PSs.[151] For example, it can include reference to identifiers such as name, location data, online identifiers (including cookie identifiers and internet protocol addresses) as well as physical, physiological, genetic, mental, behavioural, cultural or social characteristics of that person.[152] Personal information under the *Privacy Act* is a less expansive concept, although considerable confusion persists about where the limits of the concept lie.[153]

Third, the *Privacy Act* distinguishes between personal information and sensitive information. Sensitive information is accorded a greater level of protection; it may only be collected with consent (unless an exception applies), and its use or disclosure are subject to stricter requirements.[154] The CDR does not make this distinction and treats all sensitive information, with consumer consent, as an integral element of data collection and disclosure.[155]

Fourth, in addition to the PSs hardwired into primary legislation, the CDR regime's rulemaking and standard setting processes in-builds a flexibility mechanism to respond to emerging privacy threats and impose additional privacy protections (provided they are consistent with the PSs).[156] No such mechanism exists under the *Privacy Act*.

Fifth, while generally consistent with the APPs, PSs in conjunction with Part 7 of the CDR Rules are considerably more specific, as evidenced, for example, by requirements relating to the open and transparent management of data,[157] notifying of the collection of data,[158] use or disclosure of

---

[151] Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) [1.307].

[152] Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) [1.107].

[153] For example, it is unclear to what extent technical, inferred information, or metadata fall under 'personal information' in the *Privacy Act*. See *Privacy Act Review* (n 134) 24, 25.

[154] *Privacy Act* (n 81) sch 1, APPs 3, 6.

[155] See also the Treasury, *Privacy Impact Assessment: Consumer Data Right* (Report, March 2019) 36.

[156] *CCA* (n 11) ss 56BC(3)(a), 56EC(1), 56EC(2). See also the Treasury (n 155) 36.

[157] Compare APP 1 with PS 1 and rule 7.2 of the *CDR Rules* (n 14).

[158] Compare APP 5 with PS 5 and rule 7.4 of the *CDR Rules* (n 14). See also *Privacy Act Review (*n 134), noting the calls to update APP 5 to 'enhance the clarity of APP 5 collection notices' and to 'encourage entities to develop them in a user-friendly, interactive and visually engaging way': at 96.

data[159] or quality of data.[160] Due to the broad, high-level nature of the APPs,[161] many of the businesses to which they apply have long struggled with their implementation. Most fundamentally, despite the guidance offered by the OAIC on what 'personal information' within the meaning of the *Privacy Act* is, considerable confusion and uncertainty persists about what types of information are covered and what it means for an individual to be 'reasonably identifiable'.[162] Likewise, entities subject to APPs lament that there is 'not enough practical clarity about what reasonable steps they should take to protect and, when necessary, destroy personal information in a way that upholds good privacy practices.'[163] The APPs thus show that the existence of a legal obligation does not necessarily give rise to an ability to follow it. In contrast, the CDR regime provides businesses with a detailed 'rule book' enhancing their ability to meaningfully translate their obligations in practice.

Still, the key achievement of the CDR framework lies in its enforcement machinery, which is significantly underdeveloped under the *Privacy Act*. While a wide range of norms under the latter regime have been identified as long ripe for a (major) revision – and are currently being considered by the Australian Attorney-General's department[164] – two issues are particularly relevant as they illuminate a stark contrast between the incentives to comply with privacy laws laid down in both regimes.

The first issue is the right of individuals to seek compensation in the courts for a breach of privacy. The *Privacy Act* places a strong emphasis on the complaint handling by the Information

[159] Compare APP 6 with PS 6 and rules 7.5-7.7 of the *CDR Rules* (n 14).

[160] Compare APP 10 with PS 11 and rules 7.10-7.10A of the *CDR Rules* (n 14).

[161] As noted by the OAIC, the APPs are principles-based law designed broadly to enable businesses with diverse needs and business models flexibility in implementation: OAIC (n 87) para A.7.

[162] *Privacy Act* (n 81) s 6(1). See also *Privacy Act Review* (n 134).

[163] Compare APP 11 with PS 12, rule 7.11, and schedule 2 of the *CDR Rules* (n 14), and compare at APP 13 with PS 13 and rules 7.14-7.16. See also *Privacy Act Review* (n 134) 221.

[164] The review of the *Privacy Act* commenced in October 2020, instigated by an ACCC report which made a number of privacy-related recommendations: ACCC, *Digital Platforms Inquiry* (Final Report, June 2019). On 16 February 2023, the Attorney-General publicly released the Privacy Act Review Report: *Privacy Act Review* (n 134). Views are currently being sought to inform the Australian Government's response to the report.

Commissioner ('IC'). Where an act or practice of an APP entity[165] constitutes 'an interference with the privacy' of an individual,[166] the affected individual can submit a complaint for conciliation by the IC.[167] If following investigation by the IC a complaint is considered substantiated, the IC may determine remedial actions, such as directing an entity to ensure that its acts or practices interfering with the privacy do not repeat or continue, or declare that an individual is entitled to a specified amount of compensation.[168] While complainants may apply to the Federal Court or the Federal Circuit and Family Court of Australia ('FCFCOA') for an order enforcing a determination by the IC, there is no avenue for individuals to seek damages in the courts for breaches of the APPs.[169] Even where the IC determines that the complainant is entitled to compensation, the compensatory amounts awarded by the IC so far have been rather moderate and the number of determinations issued by the IC in relation to the overall volume of privacy complaints lodged annually almost negligable.[170] That the *Privacy Act* hardly offers adequate enticements for entities to respect privacy laws is, perhaps, best illustrated by the number of determinations issued in the financial year 2021-22: 17 determinations touted as a *record number* of annual determinations amongst 2,203 resolved privacy complaints.[171] In contrast to the *Privacy Act*, the CDR's deterrence mechanism is much stronger. It gives consumers the **statutory (direct) right of action**: a person who suffers loss or damage by an act or omission of another person in contravention of the CDR's PSs or the CDR Rules 'may recover the amount of the loss or damage by action against that other person or against any person involved in the contravention'.[172] Consumers could also seek to resolve disputes by recourse to a recognised external dispute resolution scheme.[173]

---

[165] Defined as 'an agency or organisation': *Privacy Act* (n 81) s 6(1).

[166] *Privacy Act* (n 81) s 13(1).

[167] Ibid s 36(1).

[168] Ibid ss 52(1)(b)(ia), 52(1)(b)(iii).

[169] Ibid ss 55A(1), 60(1), 62. See also *Privacy Act Review* (n 134) 252.

[170] *Privacy Act Review* (n 134) 252.

[171] Ibid 252.

[172] *CCA* (n 11) ss 56EY, 82(1)(d).

[173] Ibid s 56DA; *Competition and Consumer (Consumer Data Right—Recognised External Dispute Resolution Schemes) Instrument 2021* (Cth).

The second issue concerns civil penalties. The *Privacy Act* has a general civil penalty only for the most egregious interferences with privacy. Specifically, section 13G of the Act provides for the IC to take civil penalty action against the entity engaged in 'serious' or 'repeated breaches' of privacy (which can apply to breaches of any APP) in the Federal Court or FCFCOA.[174] In contrast, under the statutory CDR framework, breaches of most safeguards attract civil penalties (except for PS 2) enforceable under Part 4 of the *Regulatory Powers Act* (Cth), with no requirement for breaches to be serious or repeated.[175] The CDR Rules may also provide that certain of its provisions are civil penalty provisions under the *Regulatory Powers Act*.[176] Finally, a failure by an accredited entity to comply with PSs may lead to the suspension or revocation of accreditation.[177] Combined, these measures provide much stronger incentives for the duty-bearers under the CDR to comply with PSs and mitigate risks associated with higher velocity transfers of CDR data.

6. Conclusion

The amount of digital data produced worldwide is growing at an exponential rate. According to expert projections, the volumes of data generated globally on an annual basis is expected to reach 175 zettabytes by 2025, which is a tenfold increase from the levels recorded in 2016.[178] To provide some context to this figure, assume a current high-speed internet connection of 100 Mb/s: it would take an individual approximately 450 million years to download 175 zettabytes of data.[179]

Data has become an indispensable resource in today's information society. The vitality and value of data, however, is not inherent in data but resides in the uses to which it can be put.[180] Data

[174] *Privacy Act* (n 81) s 13G(1).

[175] *CCA* (n 11) s 56EU(2); Part 4 of the *Regulatory Powers (Standard Provisions) Act* 2014 (Cth) ('Regulatory Powers Act') allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.

[176] *CCA* (n 11) s 56BL.

[177] Ibid ss 56EA, 56BH(3).

[178] State of the Edge and Seagate, *Data at the Edge* (Report Spring 2019) 5, 7.

[179] David Reinsel, John Gantz and John Rydning, *The Digitization of the World from Edge to Core* (International Data Corporation White Paper, November 2018) 3, 7. See also 'Worldwide Broadband Speed League 2021', *cable.co.uk* (Data Map) <https://www.cable.co.uk/broadband/speed/worldwide-speed-league>.

[180] Luciano Floridi, *Information: A Very Short Introduction* (Oxford University Press, 2010) 90. ACS, *Data Sharing Frameworks* (Technical White Paper, September 2017) 21 <https://www.acs.org.au/insightsandpublications/reports-publications/data-sharing-frameworks.html>.

collected from healthcare systems, for instance, can be used to develop new drugs, identify medical conditions, and inform public health policies. In the financial sector, data can be analysed to identify patterns and trends that can be used to assess credit risk, inform investment decisions, and predict market movements.

To realise the full potential of data, it should not be siloed. Data defies boundaries and wants to move freely. Given the non-rivalrous nature of data – meaning that the same data can be used by multiple parties simultaneously in different ways – data can be leveraged to generate insights and drive innovation and competition across various industries and economy sectors. It is therefore vital, that the Australian Government resumes the roll-out of the CDR to telecommunications, insurance and superannuation and keeps expanding the regime to other economy sectors as soon as practicable.

Today, the CDR regime is world leading. The successful development of the digital economy in Australia requires that Australia maintains this lead, as the number of competitors in data-driven innovation keeps growing. UK's National Data Strategy, for example, projects a future in which the UK is 'a world leader in data' and 'a nation of digital entrepreneurs, innovators and investors, the best place [globally] to start and grow a digital business, as well as the safest place in the world to go online'.[181] The EU's ambition, by 2030, is for 'the EU to become the most attractive, most secure and most dynamic data-agile economy in the world – empowering Europe with data to improve decisions and better the lives of all of its citizens.'[182]

The task of maintaining leadership among digital economies is challenging. It requires finding a delicate balance: devising a data sharing regime which rigorously protects consumer data and ensures the system's trustworthiness, without imposing regulatory burdens that could deter new

[181] Department for Digital, Culture, Media & Sport, UK Government, *National Data Strategy* (Policy Paper, 9 December 2020) <www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy>. See also Department for Digital, Culture, Media & Sport, UK Government, 'Consultation Outcome: Government Response to the Consultation on the National Data Strategy', *gov.uk* (Web Page, 18 May 2021) <https://www.gov.uk/government/consultations/uk-national-data-strategy-nds-consultation/outcome/government-response-to-the-consultation-on-the-national-data-strategy>.

[182] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data* (Communication Working Paper COM(2020) 66 final, 19 February 2020) 6.

market entrants and stifle innovation. Given the fast pace of technological developments, the regime promises to remain a 'living document' subject to frequent revisions and updates, yet its fundamental building blocks are meant to endure. Just as filters in a water supply system are subject to quality control standards to ensure the safety of the water, the CDR data standards serve to ensure consistent and secure handling of data. The stringent accreditation requirements ensure 'the water' in this digital ecosystem is supplied by and transferred only between providers that are trusted. Consumer consent serves as 'valves' that determine 'if' the data should flow and 'to where'. The PSs fulfil important data quality and hygiene functions: they ensure that the data coming in the system is reliable, treated properly once in the system, and disposed of appropriately where no longer needed.

We believe that thinking of the CDR as a water supply and sanitation system for Australia's digital economy shows how fundamentally transformative and vital this regime will be for Australia. By raising and empowering a new generation of 'smart customers' who understand the value of their data, CDR has the real chance to radically change the competition landscape in Australia, particularly in sectors which today lack competition. Ultimately, the benefits of the CDR will accrue to all, businesses and consumers alike.