INTERNET POLICY REVIEW
Journal on internet regulation

Volume 8 | Issue 2

Citizen or consumer? Contrasting Australia and Europe's data protection policies

James Meese
IKM and Digital Studies, University of Technology Sydney, Australia

Punit Jagasia
University of Technology Sydney, Australia

James Arvanitakis
Western Sydney University, Australia

Published on 30 Jun 2019 | DOI: 10.14763/2019.2.1409

Abstract: This paper examines how data access and transfer rights are conceptualised in the European Union and Australia. The study discusses the planned introduction of a Consumer Data Right (CDR) to Australia and contrasts it to comparable developments in European law. We then assess the broader reform moments around data (which these various data access and transfer rights form a part of), that have occurred in each jurisdiction. The paper shows that Europe has placed an increasing value on protecting the fundamental rights of citizens, whereas Australia has taken a more neoliberal approach to data, only granting individuals rights in the context of the market.

Keywords: Data access, General Data Protection Regulation, Consumer Data Right, Privacy, Data protection

Article information

Received: 26 Feb 2019 **Reviewed:** 29 May 2019 **Published:** 30 Jun 2019

Funding: This research was funded through a grant from the Australian Communications Consumer Action Network. The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/citizen-or-consumer-contrasting-australia-and-europes-data-protection-policies

Citation: Meese, J. & Jagasia, P. & Arvanitakis, J. (2019). Citizen or consumer? Contrasting Australia and Europe's data protection policies. *Internet Policy Review*, *8*(2). DOI: 10.14763/2019.2.1409

This paper is part of Transnational materialities, a special issue of Internet Policy Review *guest-edited by José van Dijck and Bernhard Rieder.*

INTRODUCTION

Governments are becoming increasingly concerned about widespread corporate data collection and the information asymmetries produced through these practices. People provide their personal data in exchange for various free services, from social media platforms to fitness apps (see Andrejevic, 2014), allowing companies to gather detailed information across their customer base. However, individuals have little to no knowledge about how their data is collected, used, stored, managed or handled. In addition to concerns around the collection of personal information, the growing importance of data as an economic good has also made legislators uneasy, with many citing 'competition' as a reason for regulation (Esayas & Daly, 2018). There is a fear that consumers could be 'locked in' to particular commercial arrangements if they are unable to transfer their valuable data to a competitor (Frieden, 2017; also see Esayas & Daly, 2018). In response, numerous jurisdictions have attempted to intervene in this state of affairs by engaging in legislative reform, with the European Union's General Data Protection Directive (GDPR) standing as the most prominent example.

The initial interest of this paper is to investigate how this reform moment has increased the visibility data access and portability provisions, through a comparative study of recent reform agendas in the European Union (EU) and Australia. This analysis compares the Australian CDR reform process to the GDPR, which features a right to access data (art. 15, GDPR) and data portability (art. 20, GDPR), and data access and portability rights found in other European legislative instruments. The most prominent of these is the reformed payment services directive (PSD 2), which allows individuals and third parties to access certain banking data. At the outset, it is important to note that all of these legislative instruments have different aims. The GDPR is a regulatory framework that covers the entire European Union. It grants new rights to individuals, represents a substantial strengthening of the Data Protection Directive (1995), which it replaces (in terms of scope and enforcement, for example) and also purports to regulate algorithms (or, in the regulation's terms, "automated decision making", Art. 22). In contrast, PSD 2 requires banks to "provide access and [...] communicate, to authorized third parties, customer and payment account information" (Omarini, 2018, p. 28), providing a framework for Open Banking in Europe. Similar directives in other sectors also empower data transfers in certain situations (see Esayas and Daly, 2018). The CDR is similar to these sector-specific directives but operates on a broader scale. It introduces a general framework that gives Australians the power to ask companies that hold data to transfer all or some of that data to a third party, which can be another company in the same sector or an adjacent business. It will be introduced on a sector by sector basis (see Explanatory Memorandum, 2018).

However, this paper also extends this initial analysis and argues that the CDR is indicative of a broader conceptual divergence that places Australia at odds with Europe (despite the fact that the CDR introduces some European 'elements' into Australian law). We pursue this argument by exploring the rhetoric around the CDR, showing how politicians and policymakers have presented the right as a solution to the problem of information asymmetry. We compare this stance to the introduction of the GDPR, which saw Europe transition from a market-oriented data protection framework to one that embraced fundamental rights and freedoms (Hijmans, 2010; 2016). We argue that these different reform moments have resulted in two separate conceptual approaches to data, with Europe increasingly focused on fundamental rights and citizenship and Australia focused on the consumer and the market. We go on to suggest that Australia needs to develop a broader conceptual foundation for its data policies and move

beyond questions of economic value and efficiency to meaningfully engage with fundamental rights and embrace stronger enforcement regimes in line with existing European policy.

We also note that while existing research has already contrasted the policy proposal for the CDR with European law (Esayas and Daly, 2018), this paper analyses what is likely to be the final legislated version of the right. The Australian Coalition (centre-right) government has been a strong advocate for the CDR and supported policy development around the right throughout the 45th Parliament (2016 – 2019). Legislation was tabled in late 2018 and a subsequent Senate (upper house) Committee recommended that the bill be passed unamended. The bill did not pass parliament before it was dissolved in preparation for a May 2019 election. However the Coalition returned to power and as a result, while minor amendments may still be made the substance of the legislation examined in this article (in the form of an exposure draft) is likely to be passed. The launch of the Consumer Data Right is likely to go ahead as planned on 1 February 2020. In addition to legislation, we have also consulted public documentation and commentary to analyse the scope and purpose of the CDR.

The paper proceeds as follows. We begin by briefly discussing the different legal philosophies that influence each jurisdiction's approach to data protection. Then we introduce the CDR and compare its operation to European data access and transfer regimes. Following this, we critique the rhetoric around the right that either promotes an equivalence to the 'European' approach to data or holds up the Australian approach as superior. Finally, we compare the separate reform trajectories in both jurisdictions and suggest that the CDR is an example of Australia's broader economic approach to data and the issue of information asymmetry, which stands in stark contrast to Europe's growing commitment to fundamental rights as part of its overarching data protection framework.

EUROPE AND AUSTRALIA: DATA RIGHTS VERSUS DATA BUREAUCRACY

A central piece of legislation regulates privacy and data protection in each jurisdiction: the GDPR in Europe and the *Privacy Act* in Australia. There are some similarities between these legal frameworks to the extent that Australia's '*Privacy Act* is based on a similar model to the EU Data Protection Directive' (Esayas and Daly, 2018, p. 188). However, the two differ in how they approach privacy conceptually. The European Union treats data protection 'as a fundamental right anchored in interests of dignity, personality, and self-determination' (Schwartz and Peifer, 2017, p.123). These rights emerge constitutionally from the Charter of Fundamental Rights (8 CFR), through a specific article focused on data protection (see also Schwartz and Peifer, 2017).

In contrast, Australian does not have a constitutional foundation for data protection. Instead, it is bound up with a suite of broader protections around privacy. Protections are available at common law through the tort of breach of confidence, which is 'centred on the management and protection of private information' (Meese and Wilken, 2014, p. 320). If a confidence between parties is breached then people can make use of the tort to protect their privacy interests - which may include their data (Richardson, 2002). However, this tort is rarely used and the *Privacy Act* stands as the central legislative (and regulatory) instrument.

Indeed, its introduction in 1988 gave Australians additional protections, a new set of privacy standards for government bodies and a complaints mechanism. A newly appointed Australian

Privacy Commissioner was made responsible for ensuring that government bodies complied with relevant legislation and administering complaints from individuals. In 2000, these standards and compliance requirements were extended to private and not-for-profit organisations that had an annual turnover of AUS$ 3 million or more (Australian Law Reform Commission, 2008). While government agencies had separate compliance requirements to private and not-for-profit organisations, all of the above bodies have had to adhere to a series of Australian Privacy Principles (APP) since 2014.[1]

Following the introduction of the Act in 1988, complaints were heard by the Privacy Commissioner (latterly called the Information and Privacy Commissioner). Today, if Australians have a complaint about data protection or privacy, they must first complain directly to the offending organisation. They can only turn to the Office of the Australian Information Commissioner (OAIC)[2] if there has been no response or they feel the reply is unsatisfactory (Meese and Wilken, 2014). Once this has occurred, the Commissioner can ask parties to undertake a specific action, seek an injunction to limit particular forms of conduct or pursue a civil penalty (Office of the Australian Information Commissioner, 2018a). While suing for breach of confidence is still an option available to people, this avenue is rarely taken and it does not address all potential data protection or privacy harms an individual might face (Lindsay, 2005; Meese and Wilken, 2014). The prominence of this statutory body has caused Australian privacy law to operate within a certain bureaucratic context, standing in contrast to the European rights-based approach.

Another important conceptual distinction is that the jurisdictions have different approaches to defining data (or information). Since the enacting of the Data Protection Directive (1995), the European Union has had a continuing interest in regulating 'personal data'. This is defined as 'any information *relating to* an identified or identifiable natural person ('data subject')' (art. 2 (a) DPD or art 4.1 GDPR, our emphasis), with 'an identifiable natural person' defined as 'one who can be identified, directly or indirectly' (art. 2 (a) DPD or art 4.1 GDPR). In contrast, Australian law has only focused on protecting 'personal information', which is 'information or an opinion *about* an identified individual, or an individual who is reasonably identifiable' (see Section 6 of the Act, our emphasis). Moreover, the definition of personal information is currently undetermined, following a legal case where a journalist tried to get access to his metadata (*Privacy Commissioner v Telstra Corporation Limited,* 2017). Due to the nature of the appeal, the Full Federal Court found that personal information must be 'about an individual' but made no determination as to whether or not that included metadata. The critical issue here is that with information only needing to relate to an individual in Europe, a broader suite of data can fall under the auspices of any regulation such as data generated through an individual's use of a service. Conversely, Australian law has only regulated data that is expressly about an individual such as 'a person's name, address, contact details, signature, place of employment, work role' (Productivity Commission, 2017, p. 56) and so on.

Recent reform trajectories in each jurisdiction have further entrenched some conceptual distinctions. The GDPR strengthened Europe's commitment to a rights-based approach. A series of new rights were introduced, such as including the right to erasure (art. 17 GDPR) and the right to data portability (art. 20, GDPR). Some existing rights such as the right to access data (art. 15, GDPR) and the definition of 'personal data' (art. 4, GDPR) were carried over from the Data Protection Directive. These rights apply to any organisation that processes data: from airlines and pizza shops to cloud services and social media platforms (Diker Vanberg and Ünver, 2017). The GDPR also expanded the territorial scope of the regulation (art. 3, GDPR) and introduced stronger penalties for not abiding by the regulations (art. 83.2, GDPR). Much of the

popular press has framed the GDPR as a counterweight against large tech monopolies (Satariano, 2018) and the European Union has not shied away from this characterisation with parliamentarians threatening severe action for data breaches or misuse (Powles, 2018). In contrast, Australian legislators have ignored calls to introduce stronger privacy rights, maintaining a strong aversion towards individual rights or any constitutional protection of privacy. Their only improvement has been to streamline the regulatory framework in 2014 (see Meese and Wilken, 2014).

INTRODUCING THE CONSUMER DATA RIGHT

However, over the last two years the Australian government has started to take a more reformist approach towards data, calling for major reforms rather than incremental improvements. The CDR is a salutary example of this change. The right aims to give Australians more control over their data and a greater capacity to intervene in the growing data economy. While Australians have had the right to access their data under the *Privacy Act* for some time, they were only able to access their 'personal information', which as discussed above, only accounts for a small amount of the data that individuals produce every day (see Australian Privacy Principle 12). Under this existing right, while Australians can ask to receive their 'personal information' in a specific format, government bodies and companies can refuse the request (or ask to provide data in a different format) if the original request is not 'reasonable and practicable' to fulfil (Office of the Australian Information Commissioner, 2018b, 12.68). They can also charge for access in some cases. This means there is no standardised access process across Australia, making it arduous for people to effectively transfer data between providers.

The CDR proposes to change this. In addition to an individual's existing right to access their own personal information, it gives people (and businesses) the right to access and transfer data that 'relates' to them: that is, their personal data as well as data relating to the products they use. While the type of data that people can request will change depending on the sector, it is broadly expected to consist of data generated through the normal use of services, such as transaction histories (banking) or usage data (in energy or telecommunications). They can also ask a company to transfer their data to an approved third party, which can be based in Australia or overseas.

These data access and data transfer mechanisms are also expected to be provided for free in many circumstances (see Explanatory Memorandum, 2018, 1.55). Another important dimension is that data will also be standardised within sectors. Rather than the format of data provision being negotiated between an individual and a company (as per the existing Privacy Act), a Data Standards Body will 'prescribe the format of data, method of transmission and security requirements for data' (Explanatory Memorandum, 2018, 1.270), which data holders and accredited data recipients have to abide by. The right will gradually roll out across specific sectors, beginning in banking (and launching Open Banking in Australia as a result), before moving to the energy and telecommunications sectors.

The CDR provides Australians with better data protection by enhancing existing privacy protections and providing meaningful redress for individuals. The CDR introduces thirteen 'Privacy Safeguards' (Explanatory Memorandum, 2018, 1.6), which are variously applied to entities that hold and receive data and they largely align with existing Australian Privacy Principles. The fact that these safeguards apply to a broader range of data significantly enhances existing protections, at least with respect to access and portability. The safeguards are largely

regulated as part of the existing OAIC enforcement regime (discussed earlier), with the ACCC enforcing non-privacy related compliance. However, the bill also introduces a direct right of action for 'a person who suffers damage or loss [...] as a result of a breach of the Privacy Safeguards or consumer data rules about the privacy or confidentiality of CDR data' (Explanatory Memorandum, 2018, 1.461). This provision stands as a notable and uncommon embrace of individual rights by Australian legislators and in addition to the broader definition of data, sees Australia taking more of a European approach to data protection.

However, the right also differs from European law in important ways. The CDR provides a comprehensive framework for the entire economy whereas the European Union has taken a gradual sector by sector approach to supporting data transfers (see Esayas and Daly, 2018). It is unclear whether this broad approach will actually work effectively across multiple sectors, and indeed some sectors (like telecommunications) are unconvinced (Communications Alliance, 2019). There is also a heavy presumption that consumers will actively use the right, which may not actually be the case. Research on data access in Europe conducted prior to the introduction of the GDPR has found that 'certain organisations reported that they never received an access request, indicating that the right of access is rarely exercised by citizens' (Mahieu et al., 2018; Ausloos and Dewitte, 2018). A similar situation is present in Australia. An Australian Community Attitudes to Privacy Survey (Office of the Australian Information Commissioner, 2017, p. 15) found that 'just over a third (37%) of Australians are aware that they can request to access their personal information from government agencies and businesses which hold the information'. This lack of engagement with existing rights casts some doubt on the planned take up expected by policymakers and politicians.

The other interesting point of comparison is that the right also treats businesses as (rights bearing) consumers, which stands in stark contrast to the GDPR's focus on individual rights. While the original goal of the reform was to empower consumers and small businesses, the final bill expands the scope of the right dramatically. The explanatory memorandum states that a consumer can be "an identifiable or reasonably identifiable person, including a business enterprise" (Explanatory Memorandum, 2018, 1.100). This is a controversial further expansion of a supposed consumer-facing right (see Communications Alliance, 2019), which on its face grants significant data rights to major companies. The ease with which this expansion occurred, highlights the continuing inability of Australian law to grant individual citizens substantive data protection rights and minimises the goal of the original policy, which was to mitigate information asymmetry.

Indeed, this tendency to ignore (or at least, conflate) the rights of businesses and individuals underlines our broader concerns with the CDR. As noted in our introduction, what is particularly interesting for the purposes of this comparative paper, is the extent to which Australian policymakers and politicians either promote an equivalence to 'European' approach to data or hold up the Australian approach as superior. The following section shows how the CDR has been sold as a world-leading reform that essentially solves the 'data problem' for Australians. This framing is based on an unsupported belief in the power of big data (see Tene and Polonetsky, 2012), a limited understanding of the associated risks and an inaccurate framing of the Australian legislative environment (see Nissenbaum, 2017). We discuss these developments below by outlining this rhetoric and the broader political context surrounding the right.

RIGHTS AND RHETORIC: A DATA ACCESS REVOLUTION?

While various government reviews throughout the 2010s suggested introducing a data right for consumers, a workable concept only emerged through an inquiry run by Australia's peak economic advisory agency, the Productivity Commission. The Commission was tasked with investigating 'the benefits and costs of options for improving availability and use of data' (Productivity Commission, 2017, p. vi) and they undertook a study titled *Data Availability and Use*. The study approached the issue of data and information asymmetry from a largely economic perspective. Following this process, they presented two reform options: the consumer data right and a structure for sharing and releasing public and private data.

The Australian government welcomed the proposals and have committed to introducing both reforms. This is a problem as the CDR will only be introduced alongside the more controversial Data Sharing and Release bill. The latter bill seeks to allow government to compile data sets from public sector data and share this anonymised data with industry and researchers. While a detailed critique of the proposed sharing and release model and associated legislation are beyond the scope of this paper (criticisms are readily available, see Williams, 2018), it is enough to note that it aims to 'streamline the process for sharing public sector data' with the goal of providing more efficient government services, greater government transparency and better research data. However, the government wants to remove '500 existing data secrecy and confidentiality provisions across more than 175 different pieces of Australian Government legislation' (Department of the Prime Minister and Cabinet, 2018a, p. 10) to make this possible. It removes substantive protections for the benefit of researchers and government, with the promise of vague positive outcomes in the future, with the bill empowering the government to 'authorise data sharing and release' for broad purposes like 'supporting the efficient delivery of government services or government operations' (Department of the Prime Minister and Cabinet, 2018a, p. 6). As it stands, while Australians would get improved data access and transfer rights, this would be in exchange for allowing the sharing of public data between public and private organisations under a liberal risk assessment model.

The fact that the CDR is linked to a controversial open data framework that plans to remove a range of protections for public data has not influenced the rhetoric around the CDR. The Productivity Commission and the Australian Government have both pushed positive messages that present the reform as part of a world leading data framework. Around the launch of the initial report, the Commission's comments were incredibly optimistic, with reference to the CDR, simply noting that the right 'would provide greater insight and control for individuals over how data that is collected on them is used' (Productivity Commission, 2017, p.191). In comparison, the government's initial response was relatively restrained. They restricted their comments to the field of competition policy, where the right was anticipated to carry the greatest impact, noting that the right could 'drive greater competition between businesses to attract new customers and encourage new business models to unlock the value of consumer data' (Department of the Prime Minister and Cabinet, 2018b, p. 6).

However, as the CDR moved from idea to implementation the policy was imbued with greater significance. In 2018, the Productivity Commissioner Peter Harris wrote an article discussing the report and arguing that "the new consumer right will put Australia in the forefront of countries attempting to claw back community and individual control over their data" (Harris, 2018). Harris (2018) noted that the CDR was not the same as the GDPR and said that 'the GDPR may expand people's thinking'. However, he was bullish about his proposed reforms, arguing

that the economic approach taken by the Commission (which we discuss later on) was more effective 'as a first step in a better foundation for managing both the threat and the benefit [of data]', when compared to the GDPR, which only held a 'limited interest in this asset-driven focus of ours' (Harris, 2018).

The Australian government has been more cautious in their public statements and have not directly compared the CDR to developments in Europe. However, they have made strong statements about the capacity of the right to reduce information asymmetry. Public documentation from the Treasury, which has carriage of this reform, states that the CDR will improve the 'control, choice, convenience and confidence of consumers' (Treasury, 2018, p. 2). A media release from the then Treasurer (and now Prime Minister) Scott Morrison was equally positive, stating that the right will 'empower customers to use their data for their own benefit' and 'determine which data is shared, on what terms and with whom' (Morrison, 2018). These statements present implicit (and inaccurate) promises that Australians will be able to have some control over their data within the broader environment of surveillance capitalism (Zuboff, 2019), they are forced to contend with daily (as opposed to the ability to access a limited subset of data from specific providers). In the above cases, policymakers and politicians respectively promote the CDR as either superior to the GDPR or as a panacea to the ongoing concerns consumers hold about information asymmetry.

However, as multiple consumer advocacy groups have noted, the CDR is not a foundational reform like the GDPR, nor does it structurally intervene in data collection. In fact, both the Consumer Policy Research Centre (2018) and the Australian Communications and Consumer Action Network (2018) have argued for the introduction of a GDPR equivalent instead. The CPRC also noted that consumers may misunderstand the scope and purpose of the right:

> Considering the establishment of the GDPR in the EU, consumers may be misled in the naming of the CDR, in that it will provide the same data rights and level of protection as the GDPR when it does not (Consumer Policy Research Centre, 2018, p. 5).

These responses from civil society groups (noted elsewhere, Goggin et al., 2019), highlight both the obvious limitations of the right as well as the broader discursive power ascribed to the right by those introducing it.

Indeed, our argument rests on the premise that the introduction of the CDR and the Data Sharing and Release Bill is an important decision in Australia's general approach to data reform. As the consumer stakeholders above have signalled, this period of reform was a critical one, where Australia could have chosen to import various features from the recent European reform process. As it stands, they have only introduced a data portability right and in doing so have implied that the reform solves more problems than it actually does. It is true that Australia has a questionable history when it comes to introducing strong privacy and data protection laws (Mann and Daly, 2018), however the Productivity Commission (and subsequently, the Australian government) were charged with having to grapple with the real social and economic issues associated with information asymmetry (even as the government are facilitating elements of it, see Mann and Daly, 2018) and decide on a suitable reform agenda.

Their choices in this regard are notable. Australia has embraced what Helen Nissenbaum (2017, p. 4) calls Big Data Exceptionalism, where policymakers simply accept large-scale data

collection and focus their 'regulatory effort' on 'data use rather than data collection'. Both the CDR and the Data Sharing and Release Act have been justified on a normative basis around 'the potential of big data to deliver benefits to individuals and societies' (Nissenbaum, 2017, p. 17). As both bills make it clear, the Australian government has taken the position that data is a resource to drive economic activity and create efficiencies rather than a fundamentally political object that relates to the rights and obligations of both individuals and government. The ultimate outcome of this is that politicians and policymakers have presented this economic approach as potentially superior to the GDPR and as the foundational philosophical framework that will drive future reforms in this area.

There are potential reform options that could be seen as a counter to this general trend. The Australian Competition and Consumer Commission (ACCC) is currently holding an inquiry into digital platforms like Facebook and Google (see also Goggin et al., 2018). Their preliminary report has proposed to strengthen the definition of consent and introduce notification and erasure rights for consumers' personal information (Australian Competition and Consumer Commission, 2018). The Australian Human Rights Commission (2018) is also reviewing how human rights and technology intersect and both inquiries will present their findings shortly. However, regardless of what final reform options are proposed, we suggest that the Australian government will continue to take a market-oriented approach to data and embrace Big Data Exceptionalism. As noted earlier, Australia has a long history of ignoring rights-based reform proposals in the area of privacy and data protection (Meese and Wilken, 2014). Moreover, even if minor changes are made (say by introducing a right to erasure), these will not form part of a uniform reform agenda based on foundational rights. Instead, they will feature as an isolated selection of rights amongst a broader data framework oriented towards the market.

THE RIGHTS OF A CITIZEN OR CONSUMER AGENCY?

The Australian government has established a clear position on data and information asymmetry through the above reform proposals. It is clear that they will approach data through a largely economic lens. In the following section, we examine the implications of this decision by comparing this philosophy with Europe's data framework. Through this analysis, we argue that these competing approaches to data affect how the rights-bearing subject is configured in each jurisdiction.

As we have already outlined Australia's approach in detail, we will begin by exploring their conceptualisation of the right-bearing subject. As might be expected, Australia takes a neoliberal approach to citizenship that only grants individuals substantive rights as consumers, as seen through the CDR. While consumer advocacy groups petitioned for a broader spectrum of rights equivalent to the GDPR (Australian Communications and Consumer Action Network, 2018; Consumer Policy Research Centre, 2018), the Australian government has chosen to proceed with a data portability right that is oriented around the consumer and positioned in the context of the market. As the public documentation and commentary from politicians and policymakers cited above makes clear, while they are all drawing on the language of rights, these rights are only applicable to the marketplace and unable to be seriously used outside of that context. Indeed, it is notable that despite ongoing petitions for an actionable right to privacy in Australia for years (see Australian Law Reform Commission, 2008; 2013), the first direct right of action is being introduced within the context of this wholly consumer-oriented framework. While this is a welcome development, it is a long way from individuals being granted fundamental rights that they can call upon irrespective of the context.

Indeed, the focus on the market over broader political concerns was evident in how the broader data framework was conceived. Both the CDR and the Data Sharing and Release Bill emerged out of a policy debate focused on economics and competition law. The Productivity Commission's original report viewed the ubiquitous availability of data and broader infrastructures of personal data collection as a natural feature of contemporary life (Couldry and Yu, 2018) and simply aimed to better embed consumers within the existing market processes surrounding data. This economic orientation is particularly clear, if we consider the fact that these reform options were also linked. This choice ultimately sets up an inequitable tradeoff with the entire reform agenda implying that protections over data held by government can be traded away for more agency in the market.

While various actors have aimed to give these reforms more import, their rhetorical efforts actually do harm by tying foundational questions around the collection, use, spread of data to an economic base and distorting the broader political context around personal data. We suggest that such an approach aligns with 'a neoliberal philosophy of government in which citizens are defined through their autonomous choices as consumers of goods, services, and information' (Cohen, 2012, p. 145), with Australians being encouraged to action data rights only in relation to the market and to limit their engagement with rights to that sphere of activity.

This consumer-focused policy-making process can be usefully compared to the introduction of the GDPR, which has presented 'the most radical challenge so far to datafication' (Couldry and Yu, 2018, p. 4474). Nick Couldry and Jun Yu argue that grounding the regulation in a recognition of fundamental rights gives 'the GDPR a different character, as a discourse, from those market-driven business discourses' (Couldry and Yu, 2018, p. 4486) and (we would add), to market-oriented policy reforms like the CDR. What is perhaps more telling, is that the European Union moved away from a market-oriented structure, in the lead up to the introduction of the GDPR.

Its predecessor, the Data Protection Directive, was introduced in 1995 with the goal of harmonising data protection across the European Union and supporting a data market across the European Union (see Hijmans, 2010; 2016). The Directive sought to balance the rights of the market and the sovereign individual rather than subsuming the individual into a broader concept of 'informational capitalism' (Castells, 2010 [1996], see also Cohen, 2012). This belief was "confirmed" in the 2010 *Commission v Germany* case heard by the European Court of Justice (see Hijmans, 2016, p. 56). On its face, the GDPR appears to support these historical goals. It is interested in maintaining economic markets and facilitating the 'free flow of personal data within the Union and the transfer to third countries and international organisations' (Recital 6, GDPR).

However, as Hielke Hijmans (2016, p. 57) points out, developments in European law have changed this balance, with the GDPR now granting more weight to data protection and fundamental rights than the 'the free movement of data'. This stems from the Treaty of Lisbon in 2009, which radically changed how data protection was approached at law. The treaty gave 'binding force to the Charter of the Fundamental Rights of the European Union' (Hijmans, 2010, p. 220), which includes a 'right to the protection of personal data'. It also included a specific article in the Treaty on the Functioning of the European Union (the TFEU) that:

> not only contains an individual right of the data subject to the protection of his or her personal data, but it also obliges the European Parliament and Council to provide for data protection in all areas of European Union law (Hijmans, 2010, p. 220).

This new rebalancing of data protection has been confirmed in 'recent case law', which has ultimately 'given a more authoritative foundation to data protection as a fundamental right, rather than as an off-shoot of the internal market' (Hijmans, 2016, p. 57). Subsequently, while the GDPR makes reference to facilitating data flows across markets, these recent reforms have ensured that the regulation's primary objective is to ensure "a high level of the protection of personal data (Recital 6, GDPR). This emphasis on protection is further evidenced later on in the regulation where it specifically notes that 'human dignity' (art. 88, GDPR) is a consideration alongside fundamental rights (see Floridi, 2016).

The European story of data protection (both in terms of protections and rights) is drastically different to the Australian one discussed earlier. The jurisdiction has moved from a balanced market-oriented framework to one where fundamental rights are of central importance. What is immediately of interest is that even when Europe viewed their data protection framework as a market-enhancing policy, fundamental rights were always part of that 'balance'. This stands in stark contrast to the CDR. While there are privacy safeguards in place, the ultimate value of the reform is presumed to be generated through a consumer's greater purchasing power and ability to better choose between commercial competitors. Conversely, the European data protection framework has always considered the needs of the citizen. Historically, this has been placed in balance with the needs of the market (and as a result of that, the consumer). However, following the Treaty of Lisbon and the introduction of the GDPR, the rights of the citizen have become paramount. As a result of this we see a stronger vision of the rights-bearing subject, with individuals being granted a set of rights associated with the political realm well beyond the confines of the market.

These differences also emerge at a practical and structural level around how legislation and regulations are conceptualised. In Australia, privacy is protected by a 'patchwork of specific legislation' (Greenleaf, 2010, p. 148). Regulation and enforcement is disjointed and confusing as a result (Meese and Wilken, 2014). Rather than solve this problem, the CDR adds to the confusion by introducing a different set of privacy standards and presenting a new cause of action. Whatever 'European-style' rights and protections are present, these only occur within the context of data access and transfer and as a result, set up a multi-tiered system of privacy protection, which has the potential to confuse businesses and consumers alike. In such a context, it is difficult to articulate an appropriate vision of a citizen with respect to data protection, where clearly demarcated rights and responsibilities are evident. Australia has simply increased the complexity of its existing privacy laws and failed to provide a clear sense of what rights people have as citizens, beyond the auspices of the market.

Conversely, while there was some concern from business when the GDPR was enacted (Powles, 2018), the scope of the reform meant that it was able to provide a baseline orientation of the European Union in relation to widespread data collection processes. The GDPR positions the Union as an actor who can intervene significantly if there is evidence of data misuse (art. 83.2, GDPR) and provides European citizens with a clearer sense of their rights and obligations in the context of growing 'datafication' (see Couldry and Yu, 2018).

The obvious answer that explains this separation is that numerous Australian governments have shown a disinterest in introducing a constitutional or statutory Bill of Rights. This has meant that Australia's 'courts do not have a convenient platform in domestic law from which to develop privacy law [incorporating data protection] as an aspect of human rights' (see Greenleaf, 2001, p. 262). However, as we argue above, whatever Australia's legal history, the recent reform moment gave the country a chance to establish its position with respect to the ongoing problem

of information asymmetry. Despite embracing some European tendencies, as a whole Australia has missed an opportunity to reshape the conversation around data protection. Instead, it has presented a limited data policy that locates the vast majority of substantive rights within the context of the market.

CONCLUSION: CONTRASTING DATA FUTURES

As we conclude this article, it is important to state that we still believe that the CDR is an interesting and innovative policy. We do not agree with the legislation as it currently stands, for the reasons outlined in the paper, but there is scope to amend it and establish a data transfer framework that is more comprehensive than the European sector-based approach. Indeed, this reform could be of interest to a jurisdiction like Europe, which already bases its approach to data protection and privacy on a human rights framework, offers a more comprehensive vision of the digital citizen and carries stronger enforcement powers. However, its introduction in Australia only complicates and confuses an already weak privacy framework.

More critically, it promises to limit the policy discussion around data. Our key concern is that the CDR has been presented as a reform that solves the 'data problem' in Australia, when it is only a data access and portability right. While the right purports to transform Australians' relationship with data it ultimately restricts this freedom to the marketplace. New and potentially useful legal tools like the new cause of action are similarly restricted, only becoming relevant when individuals engage with the CDR. As a result, it does not provide Australians with a set of foundational policies that can respond effectively to increasingly powerful data collection processes. The open question is whether a future government will reorient Australia's data policy and present a reform agenda that is grounded in a recognition for human rights and offers a vision for the rights-bearing subject beyond the market.

REFERENCES

Australian Law Reform Commission. (2008). *For your information: Australian privacy law and practice* [Report No. 108]. Canberra: Commonwealth of Australia.

Australian Law Reform Commission. (2013). *Serious Invasions of Privacy in the Digital Era* [Report No. 123]. Canberra: Commonwealth of Australia.

Andrejevic, M. (2014). Big data, big questions: The big data divide. *International Journal of Communication*, *8*, 1673–1689. Retrieved from https://ijoc.org/index.php/ijoc/article/view/2161

Ausloos, J., & Dewitte, P. Shattering One-Way Mirrors – Data Subject Access Rights in Practice. *International Data Privacy Law*, *8*(1), 4–28. https://doi.org/10.1093/idpl/ipy001

Australian Communications and Consumer Action Network. (2018). Submission to The Treasury (first round). Treasury Laws Amendment (Consumer Data Right) Bill 2018. Retrieved from https://treasury.gov.au/consultation/c2018-t316972

Australian Competition and Consumer Commission. (2018). *Digital Platforms Inquiry: Preliminary report*. Canberra: Australian Competition and Consumer Commission. Retrieved from https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/preliminary-report

Australian Human Rights Commission. (2018). *Human rights and technology issues paper*. Sydney: Australian Human Rights Commission. Retrieved from https://tech.humanrights.gov.au/sites/default/files/2018-07/Human%20Rights%20and%20Technology%20Issues%20Paper%20FINAL.pdf

Castells, M. (2010). *The rise of the network society: The information age: Economy, society, and culture* (2nd edition). Chichester; Malden, MA: Wiley-Blackwell.

Cohen, J. E. (2012). What privacy is for. *Harvard Law Review, 126*(7), 1904–1933. Retrieved from https://harvardlawreview.org/2013/05/what-privacy-is-for/

Commission v Germany, Case C-518/07, EU:C:2010:125.

Communications Alliance. (2019). Submission to the Senate Standing Committee on Economics. Treasury Laws Amendment (Consumer Data Right) Bill 2019 [Provisions]. Retrieved from https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/TLABConsumerDataRight

Consumer Policy Research Centre. (2018). Submission to The Treasury (first round). Treasury Laws Amendment (Consumer Data Right) Bill 2018. Retrieved from https://treasury.gov.au/consultation/c2018-t316972

Couldry, N., & Yu, J. (2018). Deconstructing datafication's brave new world. *New Media & Society, 20*(12), 4473–4491. doi:10.1177/1461444818775968

Department of the Prime Minister and Cabinet. (2018a). *New Australian Government Data Sharing and Release Legislation: Issues paper for consultation*. Canberra, Australia: Commonwealth of Australia.

Department of the Prime Minister and Cabinet. (2018b). *The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry*. Canberra, Australia: Commonwealth of Australia.

Diker Vanberg, A., & Ünver, M. B. (2017). The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? *European Journal of Law and Technology, 8*(1), Retrieved from http://ejlt.org/article/view/546/726

Explanatory Memorandum to the Treasury Laws amendment (Consumer Data Right) Bill 2018. Canberra: Commonwealth of Australia. Retrieved from https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6281

Esayas, S.Y. & Daly, A. (2018). The Proposed Australian Consumer Data Right: A European Comparison. *European Competition and Regulatory Law Review*, *2*(3), 187–202. doi:10.21552/core/2018/3/6

Floridi, L. (2016). On human dignity as a foundation for the right to privacy. *Philosophy & Technology, 29*(4), 307–312. doi:10.1007/s13347-016-0220-8

Frieden, R. (2017). *The Internet of Platforms and Two-Sided Markets: Legal and Regulatory Implications for Competition and Consumers*. doi:10.2139/ssrn.3051766

Goggin, G., Vromen, A., Weatherall, K., Martin, F., & Sunman, L. (2019). Data and digital rights: recent Australian developments. *Internet Policy Review*, *8*(1). doi:10.14763/2019.1.1390

Greenleaf, G. W. (2001). Tabula rasa: Ten reasons why Australian privacy law does not exist. *University of New South Wales Law Journal, 24*(1). 262–269.

Greenleaf, G. W. (2010). Privacy in Australia. In J. B. Rule & G. W. Greenleaf (Eds.), *Global privacy protection: The first generation* (pp. 141 – 173). Cheltenham: Edward Elgar Publishing. doi:10.4337/9781848445123.00009

Harris, P. (2018, July 5). Data, the GDPR and Australia's new consumer right. *The Mandarin*. Retrieved from https://www.themandarin.com.au/95351-data-the-gdpr-and-australias-new-consumer-right/

Hijmans, H. (2010). Recent developments in data protection at European Union level. In *ERA Forum, 11*(2), 219–231. doi:10.1007/s12027-010-0166-8

Hijmans, H. (2016). *The European Union as a constitutional guardian of internet privacy and data protection* (PhD Thesis, University of Amsterdam). Retrieved from https://hdl.handle.net/11245/1.511969

Lindsay, D. (2005). An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law. *Melbourne University Law Review*, *29*(1), 131–178. Available at https://law.unimelb.edu.au/__data/assets/pdf_file/0006/1708017/29_1_4.pdf

Mahieu, R. L. P., Asghari, H., & van Eeten, M. (2018). Collectively exercising the right of access: individual effort, societal effect. *Internet Policy Review*, *7*(3). doi:10.14763/2018.3.927

Mann, M., & Daly, A. (2018). (Big) Data and the North-in-South: Australia's Informational Imperialism and Digital Colonialism. *Television & New Media*, *20*(4).

doi:10.1177/1527476418806091

Meese, J., & Wilken, R. (2014). Google Street View in Australia: Privacy implications and regulatory solutions. *Media Arts Law Review, 19*(4), 305-324.

Morrison, S. (2018). *More power in the hands of consumers*. Canberra: Australian Government, The Treasury. Retrieved from http://sjm.ministers.treasury.gov.au/media-release/087-2018/

Nissenbaum, H. (2017). Deregulating collection: must privacy give way to use regulation? Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3092282

Office of the Australian Information Commissioner. (2017). Australian Community Attitudes to Privacy Survey. Canberra, Australia: Commonwealth of Australia. Retrieved from https://www.oaic.gov.au/resources/engage-with-us/community-attitudes/acaps-2017/acaps-2017-report.pdf

Office of the Australian Information Commissioner. (2018a). Guide to privacy regulatory action. Canberra, Australia: Commonwealth of Australia. Retrieved from https://www.oaic.gov.au/resources/about-us/our-regulatory-approach/guide-to-oaic-s-privacy-regulatory-action/oaic-regulatory-action-guide.pdf

Office of the Australian Information Commissioner. (2018b). Australian Privacy Principle Guidelines. Canberra, Australia: Commonwealth of Australia. Retrieved from https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/

Omarini, A. (2018). "Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future." *International Business Research 11*(9), 23-36. doi:10.5539/ibr.v11n9p23

Powels, J. (2018, May 25). The G.D.P.R., Europe's New Privacy Law, and the Future of the Global Data Economy. *The New Yorker*. Retrieved from https://www.newyorker.com/tech/annals-of-technology/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy

Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4

Productivity Commission. (2017). *Data Availability and Use. Inquiry Report*. Canberra: Commonwealth of Australia.

Richardson, M. (2002). Whither breach of confidence: A right of privacy for Australia. *Melbourne University Law Review, 26*(2), 381–395.

Satariano, A. (2018, May 24). G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog. *The New York Times*. Retrieved from https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html

Schwartz, P. M., & Peifer, K. N. (2017). Transatlantic Data Privacy Law. *The Georgetown Law Journal, 106*(1), 115–179. Retrieved from https://georgetownlawjournal.org/articles/249/transatlantic-data-privacy-law

Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property*, *11*(5), 239–273. Retrieved from https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1

Treasury, Australian Government. (2018). *Consumer Data Right*. Canberra: Commonwealth of Australia. Retrieved from https://static.treasury.gov.au/uploads/sites/1/2018/05/t286983_consumer-data-right-booklet.pdf

Williams, R. (2018, August 7). The 'Data Sharing and Release Act' is coming for your data. *Independent Australia*. Retrieved from https://independentaustralia.net/life/life-display/-the-data-sharing-and-release-act-is-coming-for-your-data,11761

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

FOOTNOTES

1. Some smaller businesses such as health service providers also have to comply with this legislative framework.

2. The OAIC is the current statutory body and is headed by the Australian Information and Privacy Commissioner.