Goggin, Gerard; Vromen, Ariadne; Weatherall, Kimberlee; Martin, Fiona; Sunman, Lucy

Article

Data and digital rights: recent Australian developments

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Goggin, Gerard; Vromen, Ariadne; Weatherall, Kimberlee; Martin, Fiona; Sunman, Lucy (2019) : Data and digital rights: recent Australian developments, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 8, Iss. 1, pp. 1-19,
https://doi.org/10.14763/2019.1.1390

This Version is available at:
https://hdl.handle.net/10419/214067

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 8 | Issue 1

Data and digital rights: recent Australian developments

Gerard Goggin
Department of Media and Communications, University of Sydney, Australia, gerard.goggin@sydney.edu.au

Ariadne Vromen
University of Sydney, Australia, ariadne.vromen@sydney.edu.au

Kimberlee Weatherall
University of Sydney, Australia, kimberlee.weatherall@sydney.edu.au

Fiona Martin
University of Sydney, Australia, fiona.martin@sydney.edu.au

Lucy Sunman
University of Sydney, Australia, lucy.sunman@sydney.edu.au

Published on 31 Mar 2019 | DOI: 10.14763/2019.1.1390

Abstract: Data privacy rights is one of the most urgent issues in contemporary digital policy. In the face of insurgent citizen activism and outcry, national governments are looking for options to address this problem - something difficult for many jurisdictions when they lack robust, responsive policy frameworks, even in the wake of the call to act represented by the European General Data Protection Regulation (GDPR). In this paper we explore two Australian developments in 2018-2019 which take up the challenge: proposals from the Australian Competition and Consumer Commission (ACCC)'s Digital Platforms Inquiry to more stringently regulate social media companies when it comes to data privacy; and the government-mandated creation of a Consumer Data Right. Both policy initiatives seek to grapple with the widening pressure to provide better public domain information, fair and effective options for users to exercise choice over how they configure technologies, and strengthened legal frameworks, enhanced rights, and better avenues redress. However, in our analysis, we find little evidence that the initiatives are joined up, or connected by any common goal of really understanding, or acting on, citizen concerns to do with data privacy threats.

Keywords: Digital rights, Citizens, Privacy, Data rights, Consumers

Article information

Received: 06 Nov 2018 **Reviewed:** 25 Jan 2019 **Published:** 31 Mar 2019

Funding: This research was funded by the University of Sydney Research Excellence Initiative (SREI) scheme.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/data-and-digital-rights-recent-australian-developments

Citation: 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

This paper is part of Practicing rights and values in internet policy around the world, a special issue of Internet Policy Review *guest-edited by Aphra Kerr, Francesca Musiani, and Julia Pohle.*

INTRODUCTION

Digital rights have become a much debated set of issues in a world in which digital communications, cultures, platforms, and technologies are key to social life (Couldry et al., 2018; Hintz, Dencik, & Wahl-Jorgenson, 2019; Isin & Ruppert, 2015).

We see this, for example, in public debates about the widespread application of biometrics systems, facial recognition, or mandatory retention of telecommunications data, strategies nominally mobilised by nation states in their pursuit of information about terrorist threats, but also in controlling political dissidence. Similarly, the widespread involvement of non-state actors in the capture, analysis and trade of personal information has heightened public fears about how corporate use of their data might affect their access to information, goods and services, and also prompted questions about discriminatory applications of automated decision-making (Eubanks, 2018). Increasingly, too, linkage and use of data by governments in decision-making, and links between state and non-state actors in the collection, use, and sharing of data elicits concerns relating to power and inequality. Governments are using data beyond the security context, and also are intimately connected with the collection and use of data by private actors (including the sharing of data with third parties).

Globally and locally, it has proven difficult for citizens to propel their governments to take action, especially given the increasing complex interplay among national (and sub-national), regional, and global laws, policies, and innovation systems when it comes to internet and associated technologies. Outcomes for consumers, citizens, civil society, business, and institutions should, at least in theory, be highly influenced by the kinds of fundamental human rights set out in longstanding international frameworks, and policed (or not policed) by institutions, such as the United Nations, and as set out in national charters of rights and rights-promoting national legislation. But both national and international institutions have been slow to grapple with and enact aspects of digital rights, even as governments and non-state actors take actions that restrict or undermine those rights. Although the technologies themselves have

facilitated some counterbalance to this effect: through the growth of new rights advocacy organisations and models enabled by digital platform, such as US-based international group Access Now (Solomon, 2018).

Adding to the challenges are the decisive roles played in communications and media by nonstate-based governance and regulation arrangements, such as the community standards and terms of service of digital platforms — which decisively shape global content regulation on social media channels. There are risks that these efforts will protect existing power relations, and deflect, and make more difficult, the activation of digital rights in the context of data tracking, collection and trading, pervasive, embedded, and automated in everyday life by digital systems.

All in all, there are long, entangled challenges as well as genealogies to digital rights (Liberty, 1999). Little surprise then that the turn to digital rights has been roundly critiqued for its incoherent and partial nature. In his notable paper, for instance, Kari Karppinen argues that the umbrella concept of "digital rights" falls short of being a coherent framework. Rather, Karppinen suggests, digital rights amounts to a diverse set of debates, visions, and perspectives on the process of contemporary media transformations (Karppinen, 2017). He proposes that we approach digital rights as "emerging normative principles for the governance of digital communication environment[s]" (Karppinen, 2017, p. 96).

Reflecting on this suggestion, we imagine that such normative principles are likely to come from existing human rights frameworks, as well as emergent conceptions and practices of rights. Some especially important issues in this regard, which theorists, activists, policymakers, and platform providers alike have sought to explore via notions of digital rights, are evolving citizen uses of platforms like Facebook, personal health tracking apps, and state e-health registers and databases, and the associated rights and responsibilities of platform users.

To explore these issues, in 2017, we conducted an Australia study of citizen uses and attitudes in relation to emerging digital technology and rights (Goggin et al., 2017), as part of a larger project on digital rights and governance in Australia and Asia (Goggin et al., 2019). Our study drew on three sources of data: a national survey of the attitudes and opinions of 1600 Australians on key rights issues; focus group discussion of related rights scenarios; and analysis of legal, policy and governance issues (Goggin et al., 2017).

In summary, our study showed that the majority of respondents are concerned about their online privacy, including in the relatively new areas of digital privacy at work. A central issue across a very high proportion of respondents we surveyed is control. Their concerns regarding control are not sufficiently addressed by availing themselves of available privacy settings and options. It appears an underlying issue is lack of knowledge about what platforms, and other core actors (such as corporations and governments) do with internet users' information, and consequent absence of any sense of control. Our findings showed considerable concern about individual privacy and data protection, and the adequacy of responses by technology corporations and governments (cf. the key report by Digital Rights Watch, 2018).

Like other studies nationally and internationally (OAIC, 2017; Ofcom, 2018; Pew 2016; Center for the Digital Future, 2017), these findings lend firm support to the need for better policy and design frameworks and practices to respond to such concerns.

Following hard on the heels of our research in 2018–2019 have been successive waves of revelations and debates about data privacy breaches. Key among these was the Cambridge Analytica/Facebook exposé (Cadwallader & Graham-Harrison, 2018; Isaak & Hanna, 2018), but

also many other well publicised and controversial issues have been raised by the data collection and sharing practices of corporations and governments, by surveillance practices, and lack of effective safeguards or accountability mechanism for citizens.

In mid-2018, expectations were raised around the world by the implementation of the European General Data Protection Regulation (GDPR), with many hoping that this law would have a decisive influence on corporate policies and practices internationally, and also jurisdictions outside the direct orbit of European polity, law, and governance.

Against this backdrop, in this paper, we reflect upon subsequent developments in Australia in data privacy rights.

In the first part of the paper, we discuss Australian policy in comparison to the European and international developments. In the second part, we discuss two contemporaneous and novel Australian policy developments initiated by the national government: a Digital Platforms Inquiry; and the development of a consumer data right.

Both policy initiatives seek to grapple with the widening pressure to provide better public domain information, fair and effective options for users to exercise choice over how they configure technologies, and strengthened legal frameworks, enhanced rights, and better avenues redress. Both also illustrate the uniquely challenging environment for digital rights in Australia.

AUSTRALIAN DIGITAL RIGHTS, PRIVACY, AND DATA PROTECTION IN INTERNATIONAL CONTEXT

The concept of rights has a long, complex, and rich set of histories, across politics, law, philosophy, and ethics –– to mention just a few key domains. Shortly after the 70th anniversary of the United Nations Universal Declaration of Human Rights in 2017, it is evident that the very idea of rights remains strongly contested from a wide range of perspectives (Blouin-Genest, Doran, & Paquerot, 2019; Moyn, 2018). The recognition of certain rights is shaped by cultural, social, political, and linguistic dynamics, as well as particular contexts and events (Erni, 2019; Gregg, 2012; Hunt, 2007; Moyn, 2010).

The way that we acknowledge, defend or pursue rights — our contemporary rights "setting" — has also been shaped by the heritage of this concept in international relations as well as local contexts, and the pivotal role that rights instruments, language and discourses, practices, and struggles play in our economic, political, and social arrangements (Gregg, 2016; López, 2018). In each country, there are particular histories, arrangements, and challenges concerning rights. In relation to our Australian setting, there is a fundamental threshold issue about the constitutional and legal status of rights (Chappell, Chesterman, & Hill, 2009; Gerber & Castan, 2013). As often observed, Australia lacks an explicit, overarching constitutional or legal framework enunciating and safeguarding rights — a gap that has led many over recent years to propose a national bill of rights (Byrnes, 2009; Erdos, 2010), and led three intermediate governments, the Victorian, Australian Capital Territory, and most recently (in 2019) Queensland governments, to develop their own human rights charters.

The Australian setting is interesting to data privacy scholarship for a range of reasons, including its status as an ambiguously placed nation across global North and South (Gibson, 1992; Mann & Daly, 2018), and between West and East (Goggin, 2008; Keating, 1996). It stands as proof

that protection for human rights is not inevitable, even in a Western liberal democracy. The absence of a bill of rights or equivalent to the European Convention on Human Rights in Australia has significant implications in this context. Not least, it arguably diminishes the quality of the discussion about rights, because, for instance, it means that Australia lacks opportunities for measured judicial consideration of acts that may breach human rights, or questions regarding the proportionality or trade-off to be drawn between, for example, national security and privacy (Mann et al., 2018). That leaves researchers, institutions, and the wider society –– including the public –– with a relatively impoverished rights discussion that is skewed by the political considerations of the day and the views of advocacy groups on all sides.

The Australian case is of particular relevance to the UK going forward, and understanding the data privacy rights evolution of kindred 'Westminster' democracies (Erdos, 2010). The UK has a *Human Rights Act*, and it has some teeth, however it lacks any constitutional bill of rights (Hunt, 2015; Kang-Riou, Milner, & Nayak, 2012) –– although this has been a longstanding proposal from some actors (Blackburn, 1999), including the Conservative Party during the 2015 UK General Election. Up to now, however, it has been possible to challenge actions in the UK via EU institutions, and the UK has been bound by specific instantiations of rights in detailed EU instruments. Owing to Brexit, the existing UK human rights arrangements look like becoming unmoored from at least some judicial systems of Europe (subject to the shape of the final arrangements) (Gearty, 2016; Young, 2017, pp. 211-254).

Notably, in recent times, it has been proactive European Union (EU) response that has gained widespread attention (Daly, 2016b). Data protection is enshrined in the Treaty on the Functioning of the EU (Article 16). The fundamental right to the protection of personal data is also explicitly recognised in Article 8 of the 2000 Charter of Fundamental Rights of the European Union, and the general right to respect for 'private and family life, home and communications' (Article 7). The EU's new GDPR (European Union, 2016) took effect in May 2018. The GDPR 'seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between [EU] Member States' (Recital 3). In part, the GDPR represents an important early effort to address the implications of large-scale data analytics and automated processing and decision-making. The implications of the GDPR for citizen rights are untested in the courts so far, but the implementation of the law has provided a focal point for a sustained academic, policy, and industry discussion of automated data processing in Europe.

In the area of privacy and data protection, Europe has played an important *normative* role (Voloshin, 2014) in Australian debates (Stats, 2015), because of its leadership in this area and the involvement of many Australian researchers, jurists, parliamentarians, policy-makers, and industry figures in engagement with European actors and trends (Calzada, 2018; Poullet, 2018; Stalla-Bourdillon, Pearce, & Tsakalakis, 2018; Vestoso, 2018). Recently, the EU's expanded emphasis on its external policy portfolio, and its capacity to serve as a more "joined-up global actor", has been theorised as a kind of "new sector diplomacy" (Damro, Gstöhl & Schunz, 2017). Already the GDPR has some global effect –– introducing compliance obligations for international organisations or businesses based outside the EU that have an establishment in the EU, that offer goods and services in the EU, or that monitor or process data about the behaviour of individuals in the EU.

Another route for this strong influence has been via joint efforts under the auspices of the OECD. A watershed here was the creation and adoption of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980/2013).

Distinguished Australian High Court judge and law reformer, the Justice Michael Kirby was the Chairman of the *OECD Expert Groups on Privacy* (1978–80) and *Data Security* (1991–2). He notes that the OECD Guidelines, and the privacy principles they contain, "profoundly influenced" the foundational 1988 Australian *Privacy Act* that remains in force today (Kirby, 1999). More recently, there is abundant evidence of the influence of European law and policy reform on the wider region, as documented in the work Australian privacy scholar, Graham Greenleaf, notably his comparative study of Asian data privacy laws (Greenleaf, 2014).

Europe is thus a lodestone and an internationally respected point of reference for privacy and data protection, including in Australia. Yet, European developments also offer a stark contrast to the situation in Australia, where, in recent years, Australia's law-makers have been slow to respond to expressions of citizen and user data privacy concerns (Daly, 2016a; Daly, 2018).

STATE OF PLAY OF DATA PRIVACY IN AUSTRALIA: A SNAPSHOT

Australian privacy law is the result of both legislation and the common law. There is no right to privacy enshrined in the Constitution. Information collection and processing by government and by larger private sector players is governed by the *Privacy Act 1988* (Cth) and a range of state and territory legislation. These instruments do not, however, provide an enforceable right to privacy. The Privacy Act includes 13 Australian Privacy Principles (APPs) that impose obligations on government and private sector organisations (with some important exclusions) when collecting, handling, storing, using, and disclosing personal information, and certain rights for individuals to access and correct personal information. The Privacy Principles place more stringent obligations on entities that handle "sensitive information" about an individual, including information about their health and biometric data, racial or ethnic origin, political opinions and membership, religious beliefs or affiliation, sexual orientation, and criminal record. Both the current Australian legal framework and the terms and conditions applied by online platforms are based on a model of notice and consent: notification that personal information is being collected and consent to those users. Yet as our 2017 study indicated, even where citizens may have assented to their data collection, and may be taking active steps to protect their privacy, they are still worried that they lack knowledge of its potential uses, and control over the acquisition of personal information.

Australians, however, have no direct right to sue for a breach of the principles –– only rights to complain, first to the organisation involved or, if there is no satisfactory response, to the Office of the Australian Information Commissioner (OAIC). For its part, the OAIC's powers include "investigating individuals' complaints [in the second instance] and commencing Commissioner initiated investigations, making a determination about breaches of privacy, and applying to the Federal Court for a civil penalty order for serious or repeated interferences with privacy" (OAIC, 2018). The role, powers, and resourcing of the OAIC and its failure to take enforcement actions have been the subject of considerable criticism (Australian Privacy Foundation, 2018; Daly, 2017).

Australians' rights against unwanted intrusions on seclusion, or the unwanted revelation of private information, are also limited. The appellate courts in Australia do not currently recognise any civil cause of action for invasion of privacy, although the High Court has left open the possibility of developing one (Daly, 2016a). There is some potential to seek remedies for

serious invasions of privacy through other legal mechanisms, such as legal rights to prevent physical invasion or surveillance of one's home, rights against defamation or the disclosure of confidential information, or even copyright law (ALRC, 2014). Proposals to recognise a statutory cause of action from the Australian Law Reform Commission have not been acted on (Daly, 2016a).

None of these various Australian legal regimes have responded to broader shifts in the capacity to gather data on a larger scale, to link datasets, to analyse and pattern data, and to use such capacities to draw inferences about people or tailor what people see or the decisions that are made about them at an ever more fine-grained level (despite relatively recent 2014 reforms, cf. Von Dietze & Allgrove, 2014). For now, Australians' hope of some data protection may be indirect, via the rising tide of the GDPR and European-influenced international frameworks.

As charted by Australian privacy law expert and advocate Professor Graham Greenleaf, there is also an emergence of an effective global standard, due to widespread adoption of standards in accordance with global Data Protection Convention 108/108+ (COE, 2018; Greenleaf, 2018a & 2018b), the Council of Europe data protection convention that includes many of the GDPR requirements –– what Greenleaf terms "GDPR-lite" (Greenleaf 2018a; Kemp, 2018). Article 27 makes the Convention open to "any State around the globe complying with its provisions" (COE, 2018, clause 172, p. 32).

In October 2018, Joseph A. Cannataci, the UN Special Rapporteur on the right to privacy recommended that member states of the United Nations "be encouraged to ratify data protection Convention 108+ ….[and] implement the principles contained there through domestic law without undue delay, paying particular attention to immediately implementing those provisions requiring safeguards for personal data collected for surveillance and other national security purposes" (Cannataci, 2018, recommendation 117.e). This is a recommendation which chimes with the positions taken by Australian privacy and civil society groups — and it will be interesting to see if it is picked up by a current Australian Human Rights Commission inquiry underway on technology and human rights, expected to report in 2019 (AHRC, 2018).

The policy and legal lacunae in Australia become evident when governments and corporations are in a tense dance to reconcile their interests, in order to make the market in consumer data, sharing, and collection work smoothly and to promote innovation agendas in IT development. At the heart of the contemporary power, technology, and policy struggles over data collection and uses are citizen and user disquiet and lack of trust about the systems that would provide protection and safeguards, and secure privacy and data rights.

In Australia, there have been a range of specific incidents and controversies that have attracted significant criticism and dissent by a range of activist groups. Concerns have been raised, in particular, by policy initiatives, such as internal moves to facilitate broader government data sharing, among agencies, as well as wider, security-oriented reforms centring on facial recognition (Mann et al., 2018). One of the most controversial initiatives was the botched 2017 introduction of a national scheme called "My Health Record" to collect and make available to health practitioners the data of patients. (Smee, 2018). Such was the widespread opposition and opting-in that by February 2019, approximately 2.5 million Australians (of a population of 25 million) had chosen to opt out (Knaus, 2019).

TWO APPROACHES TO DIGITAL RIGHTS

As we have indicated, in Australia while there is a groundswell of concern and continuing activism on digital rights issues, there is no real reform of general privacy and data protection laws afoot. Instead, privacy is being addressed at a legislative level in a piecemeal way, with tailored rules being included in legislation for specific, data-related policy initiatives. Two interesting and significant initiatives underway that could, if implemented properly, make important contributions to better defining and strengthening privacy and data rights.

DIGITAL PLATFORMS INQUIRY

One important force for change is the Digital Platforms Inquiry being undertaken by the general market regulator, the Australian Competition and Consumer Commission (ACCC).

Established in December 2017 by then Treasurer, later Prime Minister the Hon Scott Morrison MP to the ACCC, the Digital Platforms Inquiry was first and foremost focused on the implications for news and journalistic content of the emergence of online search engines, social media, and digital content aggregators.

In its preliminary report, released in December 2018, the ACCC gave particular attention to Google and Facebook, noting their reliance on consumer attention and consumer data for advertising revenues as well as the "substantial market power" both companies hold in the Australian market (ACCC, 2018b, p. 4).

What is especially interesting in the ACCC's interim report and its public discussion is the salience given to issues of consumer data collection and consumers' awareness of these practices and their implications (note the framing of Australians as consumers, rather than citizens, a point to which we return below). The ACCC also found that consumers were troubled by the scale and scope of platform data collection. It also noted that they "are generally not aware of the extent of data that is collected nor how it is collected, used and shared by digital platforms" (p.8) due to the length, complexity, and ambiguity of platform terms of service and privacy policies, and that they had little bargaining power compared to platforms which largely set the terms of information collection, use and disclosure on a bundled or 'take it or leave it' basis (p.8). Reflecting on this, the ACCC argued that this information asymmetry and power imbalance had negative implications for people's capacity to demonstrate consent and exercise choice (ACCC, 2018b, p. 8). The ACCC also noted the absence of effective mechanisms for enforcing privacy laws, and cautioned that:

> The lack of both consumer protection and effective deterrence under laws governing data collection have enabled digital platforms' data practices to undermine consumers' ability to select a product that best meets their privacy preferences. (ACCC, 2018b, p. 8)

The ACCC's Preliminary Report proposes various recommendations for legislative and policy change to address issues of market power and safeguarding competition, and also proposes a set of amendments to the Privacy Act "to better enable consumers to make informed decisions in relation to, and have greater control over, privacy and the collection of personal information" (ACCC, 2018b, p. 13).

Among other things, these recommendations include: strengthening notification requirements for collection of consumers' personal information by their platform or third party; requiring that consent be express (and opt-in), adequately informed, voluntarily given, current, and specific; enabling erasure of personal information; increasing penalties for breach; and expanded resources for the Office of Australian Information Commissioner (OAIC) to scale up its enforcement activities. (ACCC, 2018b, pp. 13-14). In addition, the ACCC recommends a new enforceable code of practice to be developed by key digital platforms and the OAIC, to "provide Australians with greater transparency and control over how their personal information is collected, used and disclosed by digital platforms" (ACCC, 2018b, p, 14). Also notable is a recommendation for the introduction of a statutory cause of action enabling individuals to take action over serious invasions of privacy "to increase the accountability of businesses for their data practices and give consumers greater control over their personal information" (ACCC, 2018b, p. 14).

With the full report due in mid-2019, and formal government response to follow, a wide range of actors debated potential regulation of digital platforms, including civil society, academia, as well as industry. For their part, affected platform operators Google and Facebook were notably united in their opposition to a new regulator that could ensure greater transparency and oversight in the operation of algorithms that "determine search results and rank news articles in user feeds" (Duke & McDuling, 2019; cf. Ananny & Crawford, 2016; Google, 2018).

The international stakes are also high, illustrated in the ACCC's call for its international counterparts to follow its lead in this "world first" inquiry in applying tougher safeguards (Duke & McDuling, 2018; Simons, 2019). Pitted against the digital platform giants are the older media companies still with significant interests in press, broadcasting, and radio, supporting the call for tighter regulation of the 'digital behemoths' (Swan, Vitorovich, & Samios, 2019). Clearly protectionism of existing media market dispensations is to the fore here, rather than protection of citizen rights — these traditional corporate players are very happy to see emergent internet and digital platform companies regulated as if these were media companies; or indeed facing extensions of other regulations, such as privacy and data law and regulation.

CONSUMER DATA RIGHT: "DATA AS AN ASSET"

There has been something of a long-term, bipartisan consensus shared by both major political parties — the conservative Liberal/National Party Coalition government as well as the typically more social democratic Australian Labor Party (ALP, currently in opposition) — that, especially when it comes to internet, telecommunications, social media, and associated digital technologies, "light touch" market-oriented regulation is to be favoured. The dominant position of the ALP is to style itself as pro-market with an admixture of government intervention and responsive regulation as needed. Hence it has been generally more responsive to calls for privacy and data rights improvements, when it comes to abuses from digital platform companies. However, it is extremely reluctant to be seen as "weak" or "soft" on issues of national security, cybersecurity, and fighting terrorism, so has rarely challenged contentious Coalition laws on metadata, and data retention (Suzor, Pappalardo, & McIntosh, 2017). Most recently, in December 2018, the ALP backed down in parliament, withdrawing its proposed amendments on legislation allowing security agencies greater access to encrypted communications (creating "backdoors" in Whatsapp, iMessage, and other "over-the-top" messaging apps) (Worthington & Bogle, 2018). Internationally, this new law was received as an "encryption-busting law that could impact global privacy", as a *Wired* magazine report put it (Newman, 2018).

On the direction of the government, the ACCC is also a key player in a second, related yet

distinct initiative to better conceptualize and enact one very particular kind of digital right, in the form of a consumer data right. Data generated by consumers in using particular technologies, and their associated products and services, often resides with, and is controlled or even owned by, the company providing it. If consumers cannot access and transfer their data from one provider to another, and especially if they cannot trust a provider to use their data in agreed ways, this makes it difficult for a competitive market to be effectively established and sustained.

Following an Open Banking Review (Australian Government, 2017), and Productivity Commission report on Data Availability and Use (Productivity Commission, 2017), the Australian government decided to legislate a Consumer Data Right. The idea of this Consumer Data Right is to "give Australians greater control over their data, empowering customers to choose to share their data with trusted recipients only for the purposes that they have authorised" (Australian Government, 2018):

> ... [W]e see the future treatment of data as joint property as a healthier foundation for future policy development ... [W]hat is happening today in Australia to treat data as an asset in regulatory terms is a first step in a better foundation for managing both the threat and the benefit [of data collection]. (Harris, 2018)

The Australia consumer data right has its parallels in European developments, such as data portability right under the GDPR (Esayas & Daly, 2018), although its foundation lies in consumer rights, rather than broader digital or human rights. Such a concept of a data right — as something that an individual has ownership of — is clearly bound up with the controversial debates on "data as commodity" (e.g. Nimmer & Krauthaus, 1992; Fuchs, 2012), and indeed the wide-ranging debate underway about what "good data" concepts and practices might look like (Daly, 2019). The Productivity Commission report, which provides the theoretical basis for the data right, summarizes it as follows:

> Rights to use data will give better outcomes for consumers than ownership: the concept of your data always being your data suggests a more inalienable right than one of ownership (which can be contracted away or sold). And in any event, consumers do not own their data in Australia. (Productivity Commission, 2017, p. 191)

The consumer would have the "right to obtain a machine-readable copy of their own digital data" (p. 191), however the "asset" would be a joint property:

> Consumer data would be a joint asset between the individual consumer and the entity holding the data. Exercise of the Right by a consumer would not alter the ability of the initial data holder to retain and keep using the data. (Productivity Commission, 2017, p. 191)

The government's plan is to implement the consumer data right initially in the banking, energy, and telecommunications sectors, and then to roll it out economy wide sector-by-sector (Australian Government, 2018). The ACCC was charged with developing the rules for the

consumer data right framework (ACCC, 2018a), of which it has released a preliminary version. The consumer data right framework would be nested inside the general privacy protection framework existing in Australia, especially the *Privacy Act*. This has led to criticisms — even from industry participants, such as the energy company AGL –– that the government should take the opportunity to update and strength the existing *Privacy Act* (for instance, in relation to the Australian Privacy Principles), rather than creating a separate set of privacy safeguards, in effect leading to "twin privacy regimes" that would "complicate compliance as well as the collection of consents for data sharing from consumers" (Crozier, 2019; Dept of Prime Minister & Cabinet, 2018).

What is especially interesting in this process is the role that standards play. In the long term, the government has promised the establishment of a Data Standards Body, with an Advisory Committee including representatives of data holders (such as banks, telecommunications, and energy companies), data "recipients" (such as fintech firms), and consumer and privacy advocates. The Data Standards Body would be led by an independent Chair responsible for selection of the Advisory Committee, as well as "ensuring appropriate government, process, and stakeholder engagement" (Australian Government, 2018). In the short term, for the first three years, Data61, the digital innovation arm of Australia's national science agency (https://www.data61.csiro.au/) has been appointed to lead the development of Consumer Data Standards. Some consumer-sensitive work has been conducted in this process. For instance, Data61 conducted research with approximately 80 consumers, releasing a consumer experience report (Data61, 2019, p. 4).

As the Consumer Policy Research Centre notes in their *Consumer Data and Digital Economy* report (Nguyen & Solomon, 2018), how the framework strikes a balance will be crucial: "For consumers to benefit, policy settings need to drive innovation, enhance competition, protect human rights and the right to privacy and, ultimately, enable genuine consumer choice" (CPRC, 2018). So far, however, the framework, draft rules, and policy process has been heavily criticised by the CPRC, other consumer advocacy, privacy, digital rights groups, industry participants, and parliamentarians. (Eyers, 2019).

CONCLUSION

Citizen uses of and attitudes to privacy and data are at the heart of contemporary internet and emerging technologies. Much more work needs to be done to fill out the picture on these internationally. In particular it will be important to ensure that the full range of citizens and societies are represented in research and theory. Also it is key that such work is translated into the kinds of insights and evidence shaping and woven into the often messy policy and law making, discourses, and institutional arrangements. We would hope to see serious efforts to engage with citizens regarding their understandings, expectations, and experience of digital rights and developing technologies, with a view to informing strong, responsive citizen-centred frameworks in law, policy, technology design, and product and service offerings.

Globally, there are legislative and regulatory efforts underway to respond to people's concern about developments in data collection and use, and the feeling, documented in our research and the research of others, of an absence of effective control. The European efforts such as the Convention 108+ and GDPR have been vital in the wider international scene to provide resources and norms that can help influence, guide, or, better still, structure government and corporate frameworks and behaviour.

This paper makes a case for the importance of local context. Australia is an interesting case for examining government responses to concerns about data collection and use, as a technologically advanced, Western developed nation without an effective human (or digital) rights framework. In Australia, it is notable that efforts to respond to concern have come, not in the context of an overhaul of privacy laws or digital rights generally, but via efforts, by market-oriented policy bodies (the ACCC and Productivity Commission) to make markets work better and meet the needs, and expectations, of consumers.

In the case of the Digital Platforms Inquiry, there are internationally leading reforms to frameworks on data, algorithms, and privacy rights proposed that betoken a major step forward for citizens' digital rights. Yet in play is a political and policy process in which citizen concerns and activism are allied with some actors (even potentially old media companies), while pitted against others (digital platforms companies, including those such as Google who often argue for some element of digital rights). Ultimately it will be up to the government concerned to take action, and then for the regulators and key industry interests to be prepared to lead necessary change, ensuring citizens will have a fair and strong role in shaping co-regulatory frameworks and practices.

Like the premise of the Digital Platforms Inquiry, the Consumer Data Right initiative involves designing the architecture — legal, economic, and technical — to ensure the effective and fair operation of markets in consumer data. In both initiatives undertaken by the ACCC there is a common thread — they are aligned with consumer protection, rather than citizen concerns and rights. Here the consent, labour, and legitimation of consumers is in tension, rather than in harmony, it could be suggested, with the interests of citizens (Lunt & Livingstone, 2012). At the same time, individuals' privacy rights as *citizens* seem to be missing from the debate, subsumed under an overwhelming security imperative that frames individual privacy as consistently a lower priority than broad law enforcement and national security goals.

Thus, Australia offers a fascinating and instructive instance where internet policy experiment in compartmentalised data privacy rights is being predicated and attempted. Given the story so far, we would say that it is further evidence of the imperative for strong regulatory frameworks that capture and pin together transnational, regional, national, and sub-national level and modes to address citizens mounting privacy and data concerns; at the same time, it offers yet more evidence that, at best, this remains, in Australia as elsewhere, a work in process.

ACKNOWLEDGEMENTS

We are grateful to the three reviewers of this paper as well as the editors of the journal and special issue for their very helpful feedback on earlier versions of this paper.

REFERENCES

Ananny, M., & Crawford, K. (2016). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, *20*(3), 973–989. doi:10.1177/1461444816676645

Australian Competition and Consumer Commission. (2018a, September, 12). *ACCC seeks views on consumer data rights rules framework* [Media release MR179/18]. Retrieved from https://www.accc.gov.au/media-release/accc-seeks-views-on-consumer-data-right-rules-framework

Australian Competition and Consumer Commission. (2018b). *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 Government (2018, May 9). *Consumer data right*. Canberra: The Treasury. Retrieved from https://treasury.gov.au/consumer-data-right/

Australian Government (2018). *Review into Open Banking: Giving consumers choice, convenience, and confidence*. Canberra: The Treasury. Retrieved from https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

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

Australian Privacy Foundation. (2018, August 15). *Privacy in Australia: Brief to UN Special Rapporteur on Right to Privacy*. Retrieved from https://privacy.org.au/wp-content/uploads/2018/08/Privacy-in-Australia-Brief.pdf

Blackburn, R. (1999). *Towards a constitutional Bill of Rights for the United Kingdom: Commentary and documents*. London and New York: Pinter.

Blouin-Genest, Gabriel, Doran, Marie-Christine, & Paquerot, Sylvie. (Eds.). (2019). *Human rights as battlefields: Changing practices and contestations*. Cham, Switzerland: Palgrave Macmillan.

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. March 18, 2018. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Calzada, I. (2018). (Smart) citizen from data providers to decision-makers? The case study of Barcelona. *Sustainability*, *10*(9). doi:10.3390/su10093252

Cantacci, J. A. (2018). *Report of the Special Rapporteur on the right to privacy*. (Report No. A/73/45712). General Assembly of the United Nations. Retrieved from https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/A_73_45712.docx

Center for the Digital Future. (2017). *The 2017 Digital Future Report: Surveying the Digital*

Future. Year Fifteen. Los Angeles: Center for the Digital Future at USC Annenberg. Retrieved from https://www.digitalcenter.org/wp-content/uploads/2018/04/2017-Digital-Future-Report-2.pdf

Consumer Policy Research Centre (CPRC). (2018, July 17). *Report: Consumer data & the digital economy* [Media release]. Retrieved from http://cprc.org.au/2018/07/15/report-consumer-data-digital-economy/

Couldry, N., Rodriguez, C., Bolin, G., Cohen, J., Volkmer, I., Goggin, G.,...Lee, K. (2018). Media and communications. In International Panel on Social Progress (IPSP) (Ed.), *Rethinking Society for the 21st Century: Report of the International Panel on Social Progress* (Vol. 2, pp. 523–562). Cambridge: Cambridge University Press. doi:10.1017/9781108399647.006

Council of Europe (COE). (2018). *Convention 108+: Convention for the protection of individuals with regard to the processing of personal data*. Strasbourg: Council of Europe. Retrieved from https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

Crozier, R. (2019, March 5). AGL warns consumer data data right being "rushed". *IT News*. Retrieved from https://www.itnews.com.au/news/agl-warns-consumer-data-right-being-rushed-520097

Daly, A. (2016a). Digital rights in Australia's Asian century: A good neighbour? in Digital Asia Hub (Ed.), *The good life in Asia's digital 21st century* (pp. 128–136). Hong Kong: Digital Asia Hub. Retrieved from https://www.digitalasiahub.org/thegoodlife

Daly, A. (2019). Good data is (and as) peer production. *Journal of Peer Production*, *13*. Retrieved from http://peerproduction.net/issues/issue-13-open/news-from-nowhere/good-data-is-and-as-peer-production/

Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view. *Computer Law & Security Review*, *34*(3), 477–495. doi:10.1016/j.clsr.2018.01.005

Daly, A. (2016b). *Private power, online information flows and EU law*. Oxford: Hart Publishing.

Daly, A. (2017). Privacy in automation: An appraisal of the emerging Australian approach. *Computer Law & Security Review*, *33*(6), 836–846. doi:10.1016/j.clsr.2017.05.009

Damro, C., Gstöhl, S., & Schunz, S. (Eds.). (2017). *The European Union's evolving external engagement: Towards new sectoral diplomacies?* London: Routledge.

Data61. (2019). *Consumer data standards: Phase 1: CX report*. February 20, 2019. Retrieved from https://consumerdatastandards.org.au/wp-content/uploads/2019/02/Consumer-Data-Standards-Phase-1_-CX-Report.pdf

Department of Prime Minister and Cabinet. (2018, July 4). *New Australian Government data sharing and release legislation: Issues paper for consultation*. Retrieved from https://www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation

Digital Rights Watch. (2018). *State of digital rights*. Sydney: Digital Rights Watch. Retrieved from https://digitalrightswatch.org.au/wp-content/uploads/2018/05/State-of-Digital-Rights-Media.pdf

Duke, J., & McDuling, J. (2019, March 4). Australian regulators prepare for Facebook, Google turf war. *The Age*. Retrieved from https://www.theage.com.au/business/companies/australian-regulators-prepare-for-facebook-google-turf-war-20190304-p511kg.html

Duke, J., & McDuling, J. (2018, December 10). Facebook, Google scramble to contain global fallout from ACCC plan. *Sydney Morning Herald*. Retrieved from https://www.smh.com.au/business/companies/competition-watchdog-suggests-new-ombudsman-to-handle-google-and-facebook-20181210-p50l80.html

Erdos, D. (2010). *Delegating rights protections: The rise of Bills of Rights in the Westminster World*. Oxford: Oxford University Press.

Erni, J. (2019). *Law and cultural studies: A critical rearticulation of human rights*. London and New York: Routledge.

Esayas, S. Y., & Daly, A. (2018). The proposed Australia consumer data right: A European comparison. *European Competition and Regulatory Law Review*, *2*(3), 187–202. doi:10.21552/core/2018/3/6

Eubanks, V. (2017). *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York: St. Martin's Press

Eyers, J. (2019, February 18). Labor warns consumer data right could become second "My Health" debacle. *Australian Financial Review*. Retrieved from https://www.afr.com/business/banking-and-finance/labor-warns-consumer-data-right-could-become-second-my-health-debacle-20190218-h1be3u

Fuchs, C. (2012). Dallas Smythe today: The audience commodity, the digital labour debate, Marxist political economy and critical theory. Prolegomena to a digital labour theory of value. *tripleC: Open Access Journal for a Global Sustainable Information Society*, *10*(2), 692–740. doi:10.31269/triplec.v10i2.443

Gearty, C. (2016). *On fantasy island: Britain, Europe, and human rights*. Oxford; New York: Oxford University Press.

Gibson, R. (1992). *South of the West: Postcolonialism and the narrative construction of Australia*. Bloomington, IN: Indiana University Press.

Goggin, G. (2008). Reorienting the mobile: Australasian imaginaries. *The Information Society*, *24*(3), 171–181. doi:10.1080/01972240802020077

Goggin, G., Vromen, A., Weatherall, K., Martin, F., Webb, A., Sunman, L., & Bailo, F. (2017). *Digital rights in Australia*. Sydney: Department of Media and Communications. Retrieved from http://hdl.handle.net/2123/17587

Goggin, G., Ford, M., Webb, A., Martin, F., Vromen, A., & Weatherall, K. (2019). Digital rights in Asia: Rethinking regional and international agenda. In A. Athique & E. Baulch (Eds.), *Digital*

transactions in Asia: Economic, informational, and social exchanges. London and New York: Routledge.

Google. (2019, October 19). Second submission to the ACCC Digital Platforms Inquiry. Retrieved from https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/submissions

Greenleaf, G. (2014). *Asian data privacy laws: Trade and human rights perspectives*. Oxford: Oxford University Press.

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68–92. doi:10.1093/idpl/ips006

Greenleaf, G. (2018a, May 24), Global convergence of Data Privacy standards and laws: Speaking notes for the European Commission Events on the launch of the General Data Protection Regulation (GDPR), Brussels & New Delhi, May 25 (Research Paper No. 18–56). Sydney: University of New South Wales. doi:10.2139/ssrn.3184548

Greenleaf, G. (2018b, April 8). The UN should adopt Data Protection Convention 108 as a global treaty. Submission on 'the right to privacy in the digital age' to the UN High Commission for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy. Retrieved from https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/GrahamGreenleafAMProfessorLawUNSWAustralia.pdf

Gregg, B. (2012). *Human rights as social construction*. Cambridge, UK: Cambridge University Press.

Gregg, B. (2016). *The human rights state: Justice within and beyond sovereign nations*. Philadelphia, PA: University of Pennsylvania Press.

Harris, P. (2018, July 4). Data, the European Union General Data Protection Regulation (GDPR) and Australia's new consumer right. Speech to the International Institute of Communications (IIC) Telecommunication and Media Forum (TMF), Sydney. Retrieved from https://www.pc.gov.au/news-media/speeches/data-protection

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2018). *Digital citizenship in a datafied society*. Cambridge: Polity Press.

Hunt, M. (2015). *Parliaments and human rights: Redressing the democratic deficit*. London: Bloomsbury.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56–59. doi:10.1109/MC.2018.3191268

Isin, E. F., & Ruppert, E. S. (2015). *Being digital citizens*. Lanham, MA: Rowman & Littlefield.

Kang-Riou, N., Milner, J., & Nayak, S. (Eds.). (2012). *Confronting the Human Rights Act: Contemporary themes and perspectives*. London; New York: Routledge.

Karppinen, K. (2017). Human rights and the digital. In H. Tumber & S. Waisbord (Eds.), *Routledge Companion to Media and Human Rights* (pp. 95-103). London; New York: Routledge. doi:10.4324/9781315619835-9

Keating, P. (1996). *Australia, Asia, and the new regionalism*. Singapore: Institute of Southeast Asian Studies.

Kemp, K. (2018, September 27). *Getting data right*. Retrieved from https://www.centerforfinancialinclusion.org/getting-data-right

Kirby, M. (1999). Privacy protection, a new beginning: OECD principles 20 years on. *Privacy Law & Policy Reporter*, *6*(3). Retrieved from http://www5.austlii.edu.au/au/journals/PrivLawPRpr/1999/41.html

Knaus, C. (2019). More than 2.5 million people have opted out of My Health Record. *The Guardian*. Retrieved from https://www.theguardian.com/australia-news/2019/feb/20/more-than-25-million-people-have-opted-out-of-my-health-record

Liberty (Ed.). (1999). *Liberating cyberspace: Civil liberties, Human Rights, and the Internet*. London: Pluto Press.

López, J. J. (2018). *Human rights as political imaginary*. Cham, Switzerland: Palgrave Macmillan. doi:10.1007/978-3-319-74274-8

Lunt, P., & S. Livingstone. (2012). *Media regulation: Governance and the interests of citizens and consumers*. London: Sage.

Mann, M., & Daly, A. (2018). (Big) data and the north-*in*-South: Australia's informational imperialism and digital colonialism. *Television & New Media*, *20*(4). Retrieved from doi: 10.1177/1527476418806091

Mann, M., Daly, A., Wilson, M. & Suzor, N. (2018). The limits of (digital) constitutionalism: Exploring the privacy-security (im)balance in Australia. *International Communication Gazette, 80*(4), 369–384. doi:10.1177%2F1748048518757141

Mendelson, D. (2018). The European Union General Data Protection Regulation (EU 2016/679) and the Australian My Health Record Scheme: A comparative study of consent to data processing provisions. *Journal of Law and Medicine*, *26*(1), 23–38.

Moyn, S. (2018). *Not enough: Human rights in an unequal world*. Cambridge, MA: Harvard University Press.

Murphy, K. (2018, July 31). My Health Record: Greg Hunt promises to redraft legislation after public outcry. *The Guardian*. Retrieved from https://www.theguardian.com/australia-news/2018/jul/31/my-health-record-greg-hunt-promises-to-redraft-legislation-after-public-outcry

Newman, L. H. (2018, December 7). Australia's encryption-busting law could impact global privacy. *Wired*. Retrieved from https://www.wired.com/story/australia-encryption-law-global-impact/

Nguyen, P., & Solomon, L. (2018). *Consumer data and the digital economy*. Melbourne: Consumer Policy Research Centre. Retrieved from http://cprc.org.au/wp-content/uploads/Full_Data_Report_A4_FIN.pdf

Nimmer, R. T., & Krauthaus, P. A. (1992). Information as a commodity: New imperatives of commercial law. *Law and Contemporary Problems*, *55*(3), 103–130. doi:10.2307/1191865

Office of the Australian Information Commissioner (OAIC). (2017). *Australian community attitudes to privacy survey, 2017*. Sydney: Office of the Australian Information Commissioner. 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 (OAIC). (2019). History of the Privacy Act. Retrieved from https://www.oaic.gov.au/about-us/who-we-are/history-of-the-privacy-act

Office of the Australian Information Commissioner (OAIC). (2018, April 17). *Submission on Issues Paper –– Digital Platforms Inquiry*. Retrieved from https://www.oaic.gov.au/engage-with-us/submissions/digital-platforms-inquiry-submission-to-the-australian-competition-and-consumer-commission

OECD. (1980/2013). OECD guidelines on the protection of privacy and transborder flows of personal data. Paris: OECD. Retrieved from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Ofcom. (2018). *Adults' media use and attitudes report 2018*. London: Ofcom. Retrieved from https://www.ofcom.org.uk/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes

Pew Research Center. (2016). *Privacy and information sharing*. Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/

Poullet, Y. (2018). Is the general data protection regulation the solution? *Computer Law & Security Review*, *34*(4), 773–778. doi:10.1016/j.clsr.2018.05.021

Productivity Commission. (2017). *Data availability and use* (Report No. 82). Canberra: Productivity Commission. Retrieved from https://www.pc.gov.au/inquiries/completed/data-access/report

Simons, M. (2018, December 11). The ACCC's plan to reshape the media landscape. *Inside Story*. Retrieved from https://insidestory.org.au/the-acccs-plan-to-reshape-the-media-landscape/

Smee, B. (2018, September 18). My Health Record: Big pharma can apply to access data. *The Guardian*. Retrieved from https://www.theguardian.com/australia-news/2018/sep/18/my-health-record-big-pharma-can-apply-to-access-data

Solomon, B. (2018, August 23). (2018). Open letter to Michelle Bachelet, new High Commissioner for Human Rights. *Access Now*. Retrieved from https://www.accessnow.org/cms/assets/uploads/2018/09/Open-Letter-Bachelet.pdf

Stalla-Bourdillon, S., Pearce, H., & Tsakalakis, N. (2018). The GDPR: A game changer for electronic identification schemes. *Computer Law & Security Review*, *34*(4), 784–805. doi:10.1016/j.clsr.2018.05.012

Stats, K. (2015). Antipodean antipathy: Australia's relations with the European Union. In N. Witzleb, A. M. Arranz & P. Winand (Eds.), *The European Union and Global Engagement: Institutions, Policies, and Challenges*. Cheltenham, UK: Edward Elgar (pp. 279–304).

Suzor, N. P., Pappalardo, K. M., & McIntosh, N. (2017). The passage of Australia's data retention regime: National security, human rights, and media scrutiny. *Internet Policy Review*, *6*(1). doi:10.14763/2017.1.454

Swan, D., Vitorovich, L., & Samios, Z. (2019, March 5). Media companies back ACCC on need to patrol digital behemoths. *The Australian*. Retrieved from https://www.theaustralian.com.au/business/media/media-companies-back-accc-on-need-to-patrol-digital-behemoths-google-and-facebook/

Vestoso, M. (2018). The GDPR beyond privacy: Data-driven challenges for social scientists, legislators and policy-makers. *Future Internet*, *10*(7). doi:10.3390/fi10070062

Voloshin, G. (2014). *The European Union's normative power in Central Asia: Promoting values and defending interests*. Houndsmills, UK: Palgrave Macmillan. doi:10.1057/9781137443946

von Dietze, A., & Allgrove, A.-M. (2014). Australian privacy reforms—an overhauled data protection regime for Australia. *International Data Privacy Law 4*(4), 326–341. doi:10.1093/idpl/ipu016

Worthington, B., & Bogle, A. (2018, 6 December). Labor backdown allows Federal government to pass encryption laws. *Sydney Morning Herald*. Retrieved from https://www.abc.net.au/news/2018-12-06/labor-backdown-federal-government-to-pass-greater-surveillance/10591944

Young, A. L. (2017). *Democratic dialogue and the constitution*. Oxford: Oxford University Press.