THE UNIVERSITY OF SYDNEY

Digital Rights in Australia

Gerard Goggin
Ariadne Vromen
Kimberlee Weatherall
Fiona Martin
Adele Webb
Lucy Sunman
Francesco Bailo

Digital Rights in Australia

Gerard Goggin
Ariadne Vromen
Kimberlee Weatherall
Fiona Martin
Adele Webb
Lucy Sunman and
Francesco Bailo

Published November 2017
by Departments of Media and Communications, and Government and International Relations, Faculty of Arts and Social Sciences, and the University of Sydney Law School, University of Sydney NSW 2006 Australia

A catalogue record for this book is available from the National Library of Australia

ISBN-13: 978-0-646-98077-5

The *Digital Rights and Governance in Australia and Asia* project is funded by the University of Sydney's Sydney Research Excellence Initiative (SREI).

For more information on the project, see http://digitalrightsusyd.net/.

This report is available via the Sydney eScholarship Repository, and can be downloaded from http://hdl.handle.net/2123/17587.

Contents

Notes on Authors

Gerard Goggin is Professor of Media and Communications, and ARC Future Fellow at the University of Sydney. He researches global media policy, especially Internet and mobile media, and has a longstanding interest in digital inequality, social justice, and rights. Gerard has a particular interest in disability, digital technology, and media, and is author of *Digital Disability* (2003), *Disability in Australia* (2005), and *Disability and the Media* (2015). He is leading figure in mobile communication and media research, with key publications including *Cell Phone Culture* (2006), *Global Mobile Media* (2012), and the *Routledge Companion to Mobile Media* (2014). Gerard is founding co-editor of the new journal *Internet Histories*, and the *Routledge Companion to Global Internet Histories* (2017).

Ariadne Vromen is Professor of Political Sociology in the Department of Government and International Relations, at the University of Sydney. She has undertaken extensive research on young people's political participation, including her collaborative project *The Civic Network* on how young people use social media for politics in Australia, the UK and USA. Her new book *Digital Citizenship and Political Engagement* (2017) looks at the rise of digital activism in Australian advocacy politics. Her three current projects include: an ARC DP on the rise of crowdsourced politics via online petitions and donations; and two large Sydney funded collaborative projects (SREI) on: public attitudes towards digital rights and governance; and young women's attitudes towards the future of work in Australia.

Kimberlee Weatherall is a Professor of Law at the University of Sydney Law School, teaching and researching across intellectual property law and the IP-trade nexus, with a long interest in the intersections between law and digital technologies. She has published in a range of Australian and international journals, has been invited to speak in the US, Japan, Taiwan, China, the UK, Europe, Singapore and New Zealand, and regularly gives expert evidence to Parliamentary and law reform committees. She has been a member of the Law Council of Australia IP Committee since 2006, was member of the Commonwealth Government's Advisory Council on Intellectual Property 2013-2015 and is a member of the Board of the Australian Digital Alliance. She has also taught subjects focusing on the relationship between law and the internet and, more recently, a Masters course in Information Law.

Fiona Martin is an ARC Discovery Early Career Research Award Fellow and Senior Lecturer in Convergent and Online Media at the University of Sydney. She researches the development, uses and regulation of online media technologies (internet, web, mobile and social media) in public communications, participatory media and journalism. Her ARC funded projects are *Mediating the Conversation* (DE130101267) analysing the governance of public commenting on news websites internationally, and *Sharing News Online* (LP140100148) a Linkage Project with Assoc. Professor Tim Dwyer, Share Wars and Nine News. Fiona is the co-author of *Sharing News Online* (Palgrave Macmillan, 2018) and co-author and editor of *The Value of Public Service Media: RIPE@2013* (Nordicom, 2013). She is a former broadcast and cross-media journalist, has co-authored the *Australian Community Manager's Code of Ethics*, and teaches internet studies and online journalism in the Department of Media & Communications.

Adele Webb is Research Associate with the SREI Digital Rights and Governance Project at the University of Sydney, and currently completing her PhD in the University's Department of Government and international Relations. At the nexus of political sociology and political theory, her research considers how democracy develops meaning in different contexts through history, institutions, experience and language. She is particularly interested in these dynamics in Southeast Asia, and has written academic and media publications on the political rise of Rodrigo Duterte in the Philippines. Adele has a longstanding interest in global development, social justice and corporate accountability. Between 2008 and 2012 she was director of Sydney based NGO Jubilee Australia.

Lucy Sunman is a Doctoral Candidate at the Centre for International Security Studies at the University of Sydney. Her doctoral research examines the use of social media as part of a crisis communications strategy in response to a terrorist attack. In addition to her doctoral research, Lucy is a practising solicitor with a particular interest in the nexus between human rights law and counter-terrorism.

Francesco Bailo recently obtained his PhD from the Department of Government and International Relations at the University of Sydney. His PhD thesis investigates the impacts of online talk and social-networking sites on political participation and organisations. He is interested in digital methods and particularly in the applications of network analysis and quantitative text analysis.

Acknowledgements

This report is an output of the *Digital Rights and Governance in Australia & Asia* project, funded by the University of Sydney's Sydney Research Excellence Initiative (SREI) — and we thank the Deputy Vice-Chancellor (Research), Professor Duncan Ivison, and Research Portfolio colleagues, for this innovative program and the grant award.

The chief investigators on the project are Professor Gerard Goggin, Professor Ariadne Vromen, Professor Kimberlee Weatherall, Professor Michele Ford, and Dr Fiona Martin. As Research Associate on the project, Adele Webb has made a vital contribution to its management, conduct, and conceptualisation.

The research was greatly enhanced by a workshop we convened at the University of Sydney on 18 August 2017. Many thanks to the participants for their feedback and conversation on the digital rights policy, activism, and research agenda.

Essential Media conducted the survey and focus group research that underpins the report findings, and we thank Rebecca Huntley and her colleagues, especially Chris Strods, for their excellent work and advice.

We gratefully acknowledge the important contributions to the research and this report made by Adele Webb, Lucy Sunman, and Francesco Bailo. The report was proof-read by Sue Jarvis, Miguel Yamin provided design and layout, and we thank Gianni Wise for permission to use the cover image.

Chapter 1

Executive Summary

Australians are some of the world's greatest users of social media and mobile broadband, and our nation is in the top ten globally for internet use. At a time when our use of these technologies is increasingly redefining aspects of our personal and professional lives, *Digital Rights in Australia* explores urgent questions about the nature of our rights now and into the future.

The analysis covers rights issues in four areas: privacy, profiling and analytics; government data matching and surveillance; workplace change; and freedom of expression and speech regulation. It explores the ethical and legal challenges we face in using digital, networked technologies and the debates we are having about how to best manage their transformative impacts.

Crucially this study examines the major role of private, transnational digital platforms in reshaping the way we work, study and conduct business, our interactions with government and with each other.

The program of research which generated the *Digital Rights in Australia* report has three aims:

- to assess the evolving citizen uses of digital platforms, and associated digital rights and responsibilities in Australia and Asia, identifying key dynamics and issues of voice, participation, marginalisation and exclusion;
- to develop a framework for establishing the rights and legitimate expectations which platform stakeholders—particularly everyday users—should enjoy and the responsibilities they may bear;
- to identify the best models for governance arrangements for digital platforms and for using these environments as social resources in political, social and cultural change.

This report draws 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, illustrated by case studies. The core findings are grouped in chapter order.

Privacy, Profiling, Data Analytics

- Australians are concerned about their online privacy. While two thirds of our respondents believe they personally have nothing to hide, only a small group (18%) think that more general concerns about online privacy are exaggerated.
- A majority of our respondents do not feel in control of their privacy online. While a majority take active steps to protect their privacy (67%), and have changed settings on the social media they use most often (61%), a minority (38%) felt that they can control their privacy online.
- Women experience the online world differently from men: they are more likely to agree that they actively protect their privacy online (71%, compared with 63% of men) and change their social media settings (63%, compared with 58% of men), but feel no more in control of their privacy (39%, compared with 38% of men).
- There may be a significant group for whom the answer to questions relating to privacy online are: "it depends" (this contrasts with answers about governments and privacy).
- Corporations were the major source of concern: 57% were concerned about their privacy being violated by corporations, although a substantial number were also concerned about privacy violations by government (47%) and other people (47%).
- A large majority (78%) want to know what social media companies do with their personal data.
- In the online focus group, participants' views were mixed on the use of data in targeted advertising and price discrimination. But there was a consensus that content targeting for political purposes is different: for

example, paying a social media platform to boost a negative opinion article about a rival party to users in marginal seats was seen as crossing a line.

Government Data Matching and Surveillance

- Nearly half of our respondents were concerned about government violating their privacy (47%).
- A majority are opposed to government programs for phone companies and internet service providers to keep metadata on phone calls and web use. 79% of respondents considered retention of information about phone calls to be a privacy breach. A majority (58%) were also opposed to a policy for government-mandated retention of information about internet communications.
- But a change in frame altered these numbers. When asked whether they favour *law enforcement and security agencies* being able to access metadata, the number in favour jumped up to 42% (47% opposed). Once framed as an *anti-terrorism* measure, government data-gathering about internet is supported by a majority of respondents (57%), while only 31% oppose a program described this way.
- Our findings highlight the critical importance of the framing of questions when assessing public support for data collection and sharing, and interpreting survey results.
- Respondents' attitudes towards both government collection of communications data, and government data matching programs, varied significantly depending on political identification. Respondents who identified with the Coalition were significantly more likely to support programs; identification with the Greens made a respondent more likely to oppose such programs.
- There is considerable ambivalence among the survey participants towards online government data matching programs. We found that 42% are in favour and 45% are opposed to a program that tracks citizen use of public services and benefits. Our online focus group was also sharply divided on a range of data matching scenarios put to them.

Work

- Digital privacy at work matters. Most Australians do not think employers should look at their employees' social media pages. While 37% agreed that it was acceptable for either prospective or current employers to look at *public* social media posts; only 20% agreed that it was ok for either current or prospective employers to look at *private* posts.
- High school educated, those not working in professional/skilled work, and respondents over 40, were most concerned about employers accessing their social media posts.
- Only 16% of people agreed that using social media was an important part of their job, but most workplaces (72%) they were in had a policy about using social media while at work. Most workplaces seem to recognize the everyday ubiquity of social media use and are attempting to govern it, though only 46% of respondents said their workplace had a policy on *what* they post online.
- In this terrain of unclear directions over social media at work and employers' rights to access posts, our online discussion groups reinforced that privacy boundaries are important, but also that employees needed to use their own "common sense".
- The encroachment of some new policy agendas, such as that seen in the case study of the Public Service Commission, needs to better reflect citizens' desires for digital privacy at, and from, work.
- The app driven, online gig economy presents a new space for digital rights analysis. Most respondents have heard of, but not used, a platform such as Uber, Airtasker or Deliveroo; and use is skewed towards those under 40 and the university educated.
- Australians see gig work as providing workers with more flexibility, but at the same time a majority are also concerned about the financial insecurity of this kind of work. Over 60% believe that these new forms of work need new government regulations. Yet, as shown in the case study, institutionalising fairer regulations is fraught.

Speech

- Australians are not strongly wedded to the North American ideal of absolute speech freedom online. Just over a third (37%) of those surveyed agreed that they should "be free to say and do what I want online", but 30% disagreed and a third expressed reservations about the idea. People were also less supportive of others having that absolute freedom than themselves.
- 50% of Australians agreed that everyone should have the right to online anonymity or pseudonymity, a figure that increases to 57% for those under 40 years. Around a third of younger Australians said it was more likely that they would make honest and open comment on the news, talk about sensitive topics like sexuality or question others' opinions if they had the opportunity to comment anonymously.
- Men are more likely to assert their right to free expression than women, reflecting the male dominance of everyday speech online as much as offline.
- Gender is a key variable in understanding attitudes to social media regulation. Men were less likely than women to agree with the need to remove within 24 hours instances of sexual harassment, abuse targeted at an individual, or hate speech that encourages

violence against others. Women were less supportive than men of the right to anonymity.

- While most Australians had not experienced negative impacts from risky or harmful online speech, 39% have been affected by mean or abusive remarks and 27% have had personal content posted without consent. Our case study on image-based abuse emphasises the need for law reform and educational strategies to address new privacy and speech rights breaches.
- More than was the case for either work or privacy issues, Australians agreed on the need for more regulation of online discussion environments. They flagged the need for increased involvement by social media platforms in content moderation and 'easy' complaints reporting.
- There was a perception gap between people's belief that harmful social media content was easy to get taken down, and the procedural reality that it is not always straightforward and may require regulatory intervention to persuade the host company to act, as the European Commission hate speech case study suggests.

Policy Recommendations

1. Most Australians are concerned about their privacy online and are concerned about privacy violations by corporations. Nearly half of our respondents are concerned about government invading their privacy. Australian governments and companies need to address these concerns if they want to improve trust in the online environment, and in programs to promote expanded data use.
2. Australian governments should consider taking up recommendations from recent Australian Law Reform Commission and Australian Productivity Commission inquiries, giving Australians more control over their data and more enforceable legal rights in the area of privacy.
3. Australians are concerned about use of data, and think that some use of data analytics and targeting by advertisers are beyond the pale – especially in the electoral sphere. Digital platforms must work harder to address these concerns effectively.
4. Australians are prepared to make some trade-offs between privacy and other interests. But current policy moves to collect and centralise more data – through My Health Record or a Digital ID program – look like pushing beyond what Australians are comfortable with.
5. Digital rights to privacy while at work are a major concern for Australians. Employment relations policies need to protect workers from prospective or current employers accessing their private social media data.
6. The gig economy has led to new forms of work, driven by online platforms. Australians expect to see this precarious work better regulated via targeted employment policies.
7. Australians agreed that there should be more regulation of online discussion environments. Social media platforms need to have greater involvement in content moderation and to work with government and citizens to ensure they are providing 'easy', responsive complaints reporting.
8. As significant numbers of Australians face new forms of risky and harmful speech online, government needs to explore law reform to address new privacy and speech rights breaches.
9. While Australians acknowledge that they should take responsibility for what they say online, they could use better education in media law, content regulation and public comment guidelines given their social media publishing is increasingly open to public scrutiny and may have legal and other consequences.

Chapter 2

What are Digital Rights and Why Do They Matter Now?

Introduction: The Digital Rights Challenge

The world is experiencing a fundamental transformation in the way people work, play and participate in political life. Digital platforms like Facebook, LinkedIn, WeChat and Twitter, Airtasker, and Uber are now just as central as traditional institutions to how we organize our professional and social lives. These platforms are also disrupting the ways we engage in public debate and mobilize political action, in advanced industrial societies, as well as the authoritarian states and emerging democracies of Australia and its Asian region.

Such digital disruption has consequences for individuals' capacity to engage with their world, to connect with communities of interest, and to interrogate news and ideas. On the positive side, we now have access to new channels of information and interaction that are more difficult for governments or many corporations to control. Conversely, individuals—and governments—have little say over the scope of data collection or individuals' access to services, content management or speech standards, intellectual property or consumer rights on these platforms. And it is not clear how citizens or public bodies will have effective input into the development of private platforms, run by private entities, with often opaque decision-making processes, behavioural analytics and identity profiling and data on-selling.

What is the impact of digital disruption in our region on organisation of work, social, and political life? How are activists and ordinary people in different countries using digital platforms, to what effect, and with what challenges? How successful are governments' attempts to regulate privately owned platform operation and use? What models exist for public-private governance?

In the face of these pressing questions about how we can shape and implement digital technologies, issues of rights and governance are now a political priority. So gaining a better understanding of digital rights in Australia—mapping the rights we think we have and those we might hope for—is an urgent matter. This report is a contribution to this important societal challenge.

The *Digital Rights in Australia* Report

The report is based on research undertaken by a team of social sciences and legal researchers from the University of Sydney, and is funded by the University's *Sydney Research Excellence Initiative* (SREI). This report conveys phase one of an anticipated larger project on digital rights in Asia.

The overall aims of this project are to:

- assess the evolving citizen uses of digital platforms, and associated digital rights and responsibilities in Australia and Asia, identifying key dynamics and issues of voice, participation, marginalisation and exclusion;
- develop a framework for establishing rights and legitimate expectations which platform stakeholders—particularly everyday users—should enjoy and responsibilities they may bear;
- identify the best models for governance arrangements for digital platforms and for "activating" digital platforms as social resources in different domains.

Broadly, our aim is to bring together an understanding of two things that are often seen as distinct: the new governance processes of digital platforms, working with governments and industry; and the everyday communication practices of individuals and civil society organisations.

The report is based on the first phase of our research, conducted in 2017. In this work, we bring together two elements:

- data on Australian user attitudes towards digital rights issues (gained from a national survey conducted on our behalf by Essential Media); and
- an analysis of key law, policy, regulation, and governance arrangements.

Later in this chapter, we explain our research design for phase one. Before we do, it is necessary to provide a brief introduction of how we see digital rights, indicate the kind of issues they respond to and raise, and why they are of urgent matter for everyone.

Because debates about digital rights traverse a very large, complex terrain, we chose to focus on four areas of public concern:

- *Privacy, Profiling, and Data Analytics*
- *Government Data Matching and Surveillance*
- *Work*
- *Speech*

Understanding Digital Rights

The notion of rights has a long, complex, and rich set of histories, based in politics, law, philosophy and ethics. As we celebrate the 70th anniversary of the United Nations Universal Declaration of Human Rights (UNDHR), the very idea of rights is still strongly contested from a wide range of perspectives.

We take a broad, pluralistic approach to investigating digital rights that encompasses elements such as:

- rights explicitly set out or recognized in law, policy, and regulation;
- rights ideas and practices developed and asserted by a wide range of movements, organizations, and individuals;
- rights that extend beyond traditional frameworks of states, national, regional, and international communities of countries.

The recognition of certain rights is shaped by cultural, social, political, and linguistic dynamics, as well as particular contexts and events (Hunt, 2007; Moyn, 2010; Gregg, 2012).

The ways that we acknowledge, defend or pursue rights — our contemporary rights "setting" —has also been shaped by its heritage in international relations and the pivotal role that rights instruments, rights "talk", rights practices, and rights struggles play in our economic, political, and social arrangements.

In Australia, there are particular histories, arrangements, and challenges concerning rights (Chappell, Chesterman, & Hill, 2009; Gerber & Castan, 2013). Crucially, there is a fundamental threshold issue about the constitutional and legal status of rights, as registered in proposals and debates on a bill of rights (Byrnes, 2009; Erdos, 2010).

Markets, technology design and implementation, social innovation and option, outcomes for consumers, citizens, civil society, business, and institutions are often highly influenced by the kinds of rights set out in crucial international frameworks, and policed (or not policed) by institutions, such as the United Nations, World Trade Organization, World Intellectual Property Organization, as well as domestic law, courts, and regulation.

We are also keenly aware of the emergence of non-state-based governance and regulation arrangements, which hinge on self- or co-regulatory codes of practice, or the policies of large corporate or organization actors to implicitly define, moderate, and manage particular behaviours.

Over the last three decades the emergence of digital, networked technologies into this rights scenario has generated different responses. In the early 1990s there was great concern that "cyberspace", as it was then often termed, was a lawless frontier. A key question then was: how do existing rights apply to digital technologies?

Some two decades later such concerns have heightened — as we can see with data tracking, collection and trading, now so pervasive and embedded in everyday life as to make activating privacy rights often very difficult. What have emerged as new areas where we need to think about digital rights. Consider, for instance, instances such as: the right to be forgotten (Brock, 2016), the right to universal design (Boys, 2014; Bates, Imrie, Kullman, 2016), and our right to transparency in the operation of algorithms (Pasquale, 2015), artificial intelligence, the Internet of Things (Bunz & Meikle, 2017), and smart cities.

The scope and nature of digital rights is in pressing need of clarification (Karppinen, 2017). Perhaps the most important reason for putting digital rights on the agenda at this point of technology and social transformation is to address a disconnection between two sets of interested actors and conversations.

On the one hand, there are individuals and groups who regard themselves as digital rights activists, practitioners, and researchers. Collectively, they have made highly significant, threshold contributions in drawing our attention to new locations, frameworks, and kinds of rights that are coalesced in relation to digital technologies. Key issues such advocates have emphasised include: Internet filtering; Internet shut-down; the so-called "net neutrality" debate (Daly, 2016); the threats to freedom of expression from copyright law reform and enforcement. Institutional recognition of, and support for, such digital rights has tended to come first from organizations focussing on digital technologies,

such as Internet governance organizations like the Internet Society and its various regional chapters. A criticism of such digital rights groups is that their work is not so well connected to conventional or "traditional" human rights issues.

On the other hand, there are individuals, groups and many well-established institutions devoted to political rights, especially human rights, as these have evolved in the twentieth and twenty-first centuries — especially articulated through international human rights treaties. A criticism of such rights groups is that they have been relatively slow to give credence and pay sufficient attention to the new rights frontiers that digital technologies represent.

We note here the many different debates about rights, their relevance, effectiveness, and gulf often remarked between lofty aspiration and the many difficulties of implementing and activating rights (Gaze & Hunter, 2010; Goh, Offord, & Garbutt, 2012). In particular, we are mindful of the many norms and fundamental debates about rights, especially "human" rights, about what counts as "human", and the many varieties of the "non-human" (across different species, environments, and things).

Broadly speaking, then, we want to ensure that digital rights is brought into the fold of human and others' rights debates and struggles; and that the challenges and implications of digital rights are grappled with by the full range of rights institutions and actors.

The Terrain of Digital Rights: The Overarching Issues

As digital technologies have become widely embedded across social life, there are a set of features — in some cases, still evolving — that pose challenges, as well as opportunities, for rights.

Firstly, the introduction and adoption of digital technologies themselves changes the character of key aspects of information, communication, and media, and their associated social, cultural, and legal assumptions and frameworks. These changes to the technologies, and their uses, meanings, and business models, means that new issues are raised that need to be addressed. For instance, mobile phone cameras since their introduction in 2001 have been using for snapping and sharing intimate images. Such practices have generated questions about sexting, stalking, and image-based abuse.

Secondly, the distinctive nature of digital platforms – their private ownership, public utility and transnational operation and trading – means that new ways to resolve issues often need to be created. In particular, governance, law, policy, and regulation approaches are in the process of being rethought.

Thirdly, the ecology of organizations and businesses that offer and control large parts of digital platforms offer pressing challenges. This is especially the case because in in key areas, ranging from social media platforms and future Internet and mobile media platforms through data and algorithms, and artifical intelligence to digital economy and labour, the actors range from very large private, transnational corporations, to a diverse range of micro-enterprises and individuals.

Fourthly, there are mounting challenges to traditional human rights institutions and rights and advocacy in many countries, and at the international level which make new rights proposals more difficult to champion. Set alongside this is the growth of new advocacy organizations and models, such as those enabled by digital platforms, which complicates the variety of claims being made.

Organizations have emerged to respond to tackle digital rights issues. Forerunner groups include: the US-based Electronic Frontiers Foundation (EFF), and the Australian counterpart, Electronic Frontiers Foundation (EFA) established in 1994 (https://www.efa.org.au/); various activist, grassroots-based movements, including Free, Libre, and Open Software (FLOSS), CryptoParties, Pirate Parties, Creative Commons and digital commons groups; community informatics and community technology movements; and research organizations such as the now-defunct Cyberspace Law and Policy Centre at UNSW.

Explicitly digital rights organizations include: the international group, Access Now (https://www.accessnow.org/), established in 2009; and national groups such as Pakistan's Digital Rights Foundation (https://digitalrightsfoundation.pk/); and in Australia, Digital Rights Watch, founded in 2016 (http://digitalrightswatch.org.au/).

As well as these dedicated organizations, aspects of digital rights are also addressed by a range of advocacy and rights organisations, especially:

- those engaged with or premised upon digital platforms, such as the US-based Avaaz (https://avaaz.org/), or Australian-based GetUp! (https://www.getup.org.au/);
- decentralized technology innovation models such as Wikipedia, Wikimedia, Wikileaks;
- Internet policy, governance, and advocacy bodies, such as Internet Society, and its various chapters internationally;
- Internet and society research centres and thinktanks (often affiliated with the Global Network of Internet and Society Research Centers; http://networkofcenters.net/), such as the longrunning Centre for Internet & Society, Bangalore (https://cis-india.org/), and the Hong Kong-based Digital Asia Hub (https://www.digitalasiahub.org/);

- digital inclusion groups, such as the Australian Digital Inclusion Alliance, established in 2017 (http://digitalrightswatch.org.au/).
- parliamentarians;
- media, communications, and information policy, advocacy, and research groups;
- industry groups and individual technology companies;

Some Key Areas of Digital Rights

In our report, we focus on four areas important for digital rights, and then do so only by paying attention to selected aspects of these. There are a wide range of other areas of digital rights that we will briefly note — to indicate significant issues as well as the complexity, range and scope of the digital rights terrain. In doing so, we would observe that, like other areas of rights, there are often contradictions and tensions between particular digital rights, or elements within a right. Further, that the boundary of what is and is not properly or usefully regarded as *digital* dimensions of rights is often unclear.

Internet Freedom

The advent of the Internet has progressively raised important forerunner issues of contemporary digital rights; notably via its role in enabling freedom of expression, sometimes termed "Internet freedom".

A foundational concern here is effective access to Internet, which can incorporate a range of access and inclusion dimensions. Obvious threats to Internet freedoms include various ways to shut down or disable Internet access: service blocking, denial of service attacks, content filtering, and attempts to undermine "net neutrality", or the move away from treating all Internet traffic "equally", rather than giving preference to speed and quality to some "premium" or business services).

Intellectual Property (IP)

IP is a central area of digital rights, especially because the norms of creating information in digital forms allows new kinds of controls for right holders, because copying and sharing of digital information raises new problems of rights management and because new areas of information, media, and communication have become part of the digital realm, raising new issues of ownership and rights. Debate has ensued on the appropriate way for copyright treaties and laws to acknowledge and deal with digital information and platforms, especially with the strong links copyright can have for digital economy and culture (Lessing, 2004; Lessing, 2008). Good examples of particular uses and practices that have led to debate include: downloading and sharing of digital content (such as software, music, TV and music); copyright protections on e-books; ownership of information (Fairfield, 2017) and user-generated content, which underpins social media platforms.

Internet Governance

Internet governance emerged with mechanisms and cultures to develop and coordinate technical and social operation of the Internet. From the mid-1990s to the present Internet governance developed internationally, with the establishment of bodies such as ICANN, the Internet Corporation for Assigned Names & Numbers, the World Wide Web Consortium and the Internet Engineering Task Force.

From the 2010s, the North American dominance of internet governance has been subject to widespread critique, while key concepts and forms of Internet governance have been challenged, especially multistakeholderism. Major governance gatherings such as the World Summit on the Information Society have put on the agenda the need for genuinely international Internet governance, that acknowledges the changing geopolitics of this core area of digital networks.

As well as the expanding range of issues emerging in Internet governance what the area highlights that that policy analysis, governance, and regulation are essential to understand alongside, or as building blocks of, digital rights.

Digital Citizenship

In the 1990s, digital citizenship was conceived as a new form of political participation — the need for people to develop internet literacies and understandings of networked social relations that would enable them to engage with online education and other government services, as well as accessing political information and discussion forums (Ohler, 2010; Vromen, 2017).

Over time the concept has encompassed other competencies, such as those expressed in the European Digital Framework for Citizens (European Commission, 2016a), which mandates people develop knowledge and skills in information literacy, communication and collaboration, content creation, safety and problem solving in order to fully participate in society.

Debates about the scope of digital citizenship have encompassed different conceptions of rights and responsibilities and ways to behave and interact with others, as well as various approaches to personal privacy and information security, and proposals for national data monitoring and collection.

Digital Rights for Different Actors

Integration to issues of digital digital citizenship and platforms, we also need to consider the particular rights issues for, and perspectives of, different kinds of actors – especially those whose rights, or claims to rights, has been overlooked.

Gender and sexuality are two important, complex, intersectional axes of identity, belonging, and

communities that shape digital rights notions, practices, and contexts. Despite considerable effort to advance various aspects of women's participation to digital platforms, the situation across most countries and settings remains profoundly unequal. Sexual minorities, such as LGBTQI groups, often note the benefits and new opportunities extend via digital platforms, but also the systematical barriers, harassments, and exclusion they still face.

Children are another group who have been a focus in eSafety policy, law, and education. However, children's digital rights — rather than those of their parents, carers, or families —have been relatively overlooked (Taylor & Rooney, 2016). Emergent work on children's rights in the digital age, that builds on the Convention on the Rights of the Child (CRC), for instance, is an important endeavour, and useful for general understandings of digital rights (Livingstone & Third, 2017).

People with disabilities are another large group whose digital rights go well beyond the typical, and still vital, association with web accessibility. The 2006 Convention on the Rights of Persons with Disabilities (CPRD) is a "post-Internet" Treaty that has many articles that rely upon people having full, effective, and affordable access to digital technologies.

Indigenous people are yet another group who have achieved considerable social innovation with their appropriation of and engagement with digital platforms, yet whose distinctive digital rights are often ignored. This is often the case too with a range of linguistic and cultural minorities, for whom digital platforms can provide important visibility, resources, and new communicative possibilities; yet who are often not included in digital rights conceptions.

Migrants, refugees, asylums seekers, and other displaced or migratory groups often face particular issues with digital rights. From very different perspectives, so do prisoners, where assumptions of rights often are not believed to apply, and whose lives are governed by institutions where Internet and digital technologies are circumscribed.

Four Key Rights Domains in this Report

In this report, we have chosen four priority areas for our survey of contemporary Australian concerns on digital rights: privacy; surveillance; work; and speech. There are many other important aspects of digital rights, but we selected these as they are of widespread concern.

Privacy, Profiling, and Data Analytics

Privacy is a longstanding and much debated social and legal issue. Traditional liberal notions of public and spheres are collapsing, as challenges emerge associated with digital platforms.

The nature of privacy itself continues to be discussed, not least because notions of privacy can be specific to a range of factors: cultural context; age, class, gender, sexuality, race, disability, and other categories (Taylor & Rooney, 2016); income and occupation. Regardless of one's view of privacy, it is clear that there are mounting issues in societies where: much existing kinds of information are now held in digital form; and new kinds of information, premised on digital platforms, are being created, held, and brought to bear across many aspects of everyday, private, and public life (Friedewald et al., 2017). Such issues are highlighted by incidents such as: the inadvertent release or hacking of personal and credit card information, held by businesses; the use of information gained via social media profiles and activity for purposes not intended by the person; and concerns about safety, security, and potential harassment, due to gathering of geolocation data from apps, smartphones, or WiFi. At an overarching level, the question arises more broadly of whether a unique concept of "digital privacy" needs to be developed.

Government Data Matching and Surveillance

The extent of information and data gathered through digital platforms, the development of technologies to make sense of it (especially computational technologies), and the wide range of uses organizations and government can potentially make of such data, makes surveillance a central issue (Cole, Fabbrini, & Schulhofer, 2017; Daly, 2017). Because of the wide range of data held by private organizations, especially commercial organizations, there are a greatly expanded set of ways in which individuals and groups can be surveilled. In addition, there are concerns that surveillance practices are regarded as acceptable, because of the potential benefits that may be advanced.

Surveillance of citizens, and other populations, by governments has been a longstanding concern, which has been embodied in various rights and protections. Consider, for instance, the "Five Eyes" arrangement, by which the US, UK, Australia, New Zealand, and Canada have collected and shared intelligence since the World War II period. This kind of gathering of data for intelligence purposes has been dramatically extended by new data infrastructures and collection practices (Ruby, Goggin, & Keane, 2017). In particular, telecommunications and Internet data held by private companies is routinely shared with government agencies — widespread practices that came to light with the relevations of whistle-blower Edward Snowden concerning the US National Security Agency (NSA). Governments around the world, including the Australian government, have passed legislation on data retention, interception, access, and investigation, requiring digital technology companies to make user data available. The rationale for such legislation is often cited as the presence of extended national security threats especially, after 9/11, terrorism.

The availability and cross-matching possibilities of a wide range of other data is something currently being developed by governments. In Australia, analysis of data has been advanced as ushering in a powerful new tool of welfare policy, to pinpoint and tackle areas of poverty and welfare "dependence". The stakes in such governmental uses of data were highlighted in the so-called "Robo debt" affair of 2016-2017, in which Centrelink, in its Better Management of the Social Welfare System Initiative, relied upon data matching to identify overpayment, and then on databases and automation to notify recipients and require repayment (Senate, 2017). Other important areas of surveillance include e-Health (Adams, Purtova, & Leenes, 2017), face recognition technology, and biometrics. In China, new plans for using citizens' data raise the prospect of whole of population and life-course surveillance.

Given the vast growth in surveillance, accountability, social and legal frameworks, conceptualisations of rights, identification of breaches (such as discriminatory data practices), and effective and practices for accessing rights have lagged (Norris et al. 2017).

Work

Rights at work is a longstanding area of concern for new technology. In relation to digital technologies, there are a range of potential rights' concern — many with clear precursors, and some which are much more distinctive.

The "digitalisation" of work affects most workers, however to varying degrees, and often in different ways. The processses of digitalisation have been underway since the major changes in information and communication technologies in the second half of the twentieth century, including: the heightened role of information in workplaces; the emergence of new kinds of work and professions; telecommunications and computerization, and their role in work transformations (Flecker, 2016; Fuchs, 2014).

In the past decade or so, the reliance upon workers and their organizations upon computers, Internet, mobile communication, and social media, has brought issues of digitlisation further to the fore, raising fundamental issues about the nature of work, and the relationship between work and home and other "non"-work setting (Gregg, 2011). Digitalisation of work has also been underway in the arenas of domestic work and labour, as well as other kinds of "unpaid", less official, or valorized work, such as caring and voluntary work (Wilson & Yochim, 2017).

Digital platforms have been interwoven into the creation of new forms of work and labour, moving beyond "telecommuting", "mobile office", "call centre" setting and practices into work such as: creating digital platforms or content; work in digital economy, such as creating value for sale to gamers; work supported by digital intermediary platforms (such as Airbnb; Uber; Delivero; Airtasker); and crowdwork platforms (such as Mechanical Turk) (Gahan, Healy, & Nicholson, 2017).

New developments in digital technologies, especially robotics, AI, and associated technologies, are raising concerns about the future of work.

Because of the prevalence and extension of digital platforms into many areas of work, there are new kinds of issues that are not necessarily clearly captured by labour rights. For instance, the issues of freedom of expression on social media platforms.

Digital technologies have often been associated with discourses that emphasise the new possibilities of generating flexible work, value, and other benefits from new arrangements. It has often proven difficult to ascertain, identify, and address the challenges to work-related rights issues.

Speech

Speech, expression and associated communicative rights have tended to feature in the "top table" of human rights conversations (Gelber, 2011). Digital technologies have been praised and counted upon for opening up new avenues by which people can exercise their freedom of expression, mobilise political change, problem-solve across cultural boundaries and develop creative economies. Our understanding of speech freedoms then is tightly bound with other conceptions of political, social and cultural agency, and with economic development.

The new avenues and dimensions of such digitally-enabled freedoms of expression can be threatened or curtailed, as we see above in relation to Internet freedoms. Key issues for societies to navigate include how to conceptualize and safeguard speech, expression, and communication rights, how to chart the new ethical dimensions of online communicative relations and how to encourage talk that encourages participation by all, rather than just the most vocal or privileged, and in forms of address and tone that includes, rather than excludes. These freedoms also pose new challenges for how expressive domains such as social media platforms might be regulated — not least with the rise of non-state actors, especially in the form of transnational corporations owning and providing media environments (Laidlaw, 2015; Verhulst, Price, & Morgan, 2013).

An important issue relates to the longstanding issues of balancing responsibilities and rights, especially given the interconnectedness in digital platforms, between effective expression, listening, and civility. Here the much-vaunted expansion in channels and means for people to express themselves via Internet, which raised such hope in the 1990s (and still does inspire action), can be vitiated for many with the realities of social and mobile media communication. Here new, circumscribed and visual modes of speaking present challenges for

interpretation across cultural boundaries. The possibility for anonymous and pseudonymous talk can be exploited in aggressive, even violent and exploitative ways. Even the evolution of real-name identification systems for social media systems has not stemmed the tide of aggressive and harmful speech that can deter people from participation in public discussion.

Much of the discourse around digital rights then has been occupied with strategies to help speakers protect themselves from online harassment (especially race, gender, sex, disability, and other-inflected harassment), trolling, misinformation and extortion, swatting, doxxing, and image-based abuse. In recent years however the focus has shifted to examine the broader rights setting – including the right of social media users to be free from harmful speech, and the consequent regulatory responsibilities of the host or publishing platforms, as well as governments supported by civil society organisations involved in content regulation, speech rights and civil liberties issues. Equally important are young people's rights to better education in media law, content regulation and public commenting policies as these apply to their social media use in study and work.

Research Approach and Design

As noted, this report presents phase one of a larger study of digital rights in Australia and Asia. Phase one has three methodological components: a survey; discussion group; and legal-policy analysis.

i. Survey: We commissioned Essential Media to conduct a representative survey of 1600 Australian respondents (see Appendix for the full questionnaire). The 1600 participants were randomly selected to undertake an online survey from Essential Media's *Your Source* online panel of over 100,000 members. The survey was conducted in July 2017. Essential Research provided incentives to its online panel members in the form of points. In addition, Essential Research provided a $100 incentive to the participants in the online focus group discussion.

Key themes of survey included:

- Information & Privacy: privacy violations; control; platform regulations
- Work: social media at work; future of work; gig economy
- Speech online: free speech; anonymity; online abuse; and platform responsibilities.
- Demographics: social media use; social background; partisanship.

All respondents completed the Information and Privacy sections of the questionnaire. 800 respondents complete the Work section, and 800 completed the Speech section of the questionnaire.

Throughout the report we present analysis of the digital rights attitudinal and behavioural data as cross tabulation with key demographic variables such as: gender, age, education attainment, location, frequency of social media posting, occupation type, and party identification. When there is a significant statistical difference between groups an * is used.

ii. Discussion Groups: Following the survey, participants were asked if they were willing to be contacted again to take part in an online discussion forum. Based on the criteria of being over 35-year-old males and females Australia wide, and medium to frequent users of social media, the 14 participants were randomly selected for the online discussion forum.

Scenarios used include:

- Personal data use by internet companies (e.g. targeted advertising)
- Employer and employee social media use
- Government use of personal data (e.g. tax, health, law enforcement)
- Freedom of speech, abuse, complaints and regulatory processes.

We received ethical approval for the research from the University of Sydney's Human Rights Ethics Committee (project no. 2017/461).

iii. Legal and Policy Analysis of Digital Rights and Governance Debates and Current Cases:

Following the survey and discussion group research, we chose relevant aspects of Australian and international digital right law, policy, cases, and debates for detailed research and analysis.

Chapter 3

Privacy, Profiling, Data Analytics

Core findings

- Australians are concerned about their online privacy. While two-thirds of our respondents believe they personally have nothing to hide, only a small group (18%) thinks that more general concerns about online privacy are exaggerated.
- A majority of our respondents do not feel in control of their privacy online. While a majority take active steps to protect their privacy (67%), and have changed settings on the social media they use most often (61%), a minority (38%) feel they can control their privacy online.
- Women experience the online world differently from men: they are more likely to agree that they actively protect their privacy online (71%, compared with 63% of men) and change their social media settings (63%, compared with 58% of men), but feel no more in control of their privacy (39%, compared with 38% of men).
- There may be a significant group for whom the answer to questions relating to privacy online is 'It depends' (this contrasts with answers about governments and privacy).
- Corporations are the major source of concern: 57% of respondents were concerned about their privacy being violated by corporations, although a substantial number were also concerned about privacy violations by government (47%) and other people (47%).
- A large majority (78%) want to know what social media companies do with their personal data.
- In the online focus group, participants' views were mixed on the use of data in targeted advertising and price discrimination; however, there was a consensus that content targeting for political purposes is different – for example, paying a social media platform to boost a negative opinion article about a rival party to users in marginal seats was seen to be crossing a line.

3.1 Issues in privacy and data processing in policy and practice

Digital platforms collect and use a wide range of information about their users. They collect highly granular data provided by users that directly reveals users' interests, beliefs, political orientation, personal family and social networks, location and regularly visited locations, and spending habits. Some platforms – especially comprehensive social media sites like Facebook – collect indirect information from users' interactions with pictures and news stories that may reveal these types of information or, by inference, more intimate information that users would prefer to keep private. Platforms may also collect and link information gleaned from other members of an individual's network, such as contact details held by a friend or photos uploaded and tagged by a family member (Marwick & boyd, 2014).

Increases in processing speed and power, and more advanced data analytics techniques and tools, expand the ability of online platforms to use these data to draw inferences and determine in real time what users of platforms will see. On the major social media platforms, for example, people will see a highly targeted and individualised newsfeed, generated through analysis of all the personal information that has been collected, as well as information about other users and their responses. The feed is designed to hold attention for as long as possible and increase users' interactions with the content (DeVito, 2017). Advanced techniques are being developed with the goal of increasing the likelihood that people will see advertisements that will motivate them to act – even predict what they might want before they are aware of it themselves. Large datasets collected over time can also affect other real-world outcomes – for example, to determine who will be offered certain prices or insurance rates, credit or job opportunities. Increasingly in public there is concern that such analysis

has been used to affect political discourse and even voting patterns (Tufecki, 2015).

There is a growing awareness of these issues in the mainstream media. But apparently increasing awareness of the potential risks and downsides of large-scale data collection and analytics is not leading to a decline in the use of digital platforms. People are making trade-offs between privacy and other interests, and developing strategies for managing how information about them is disclosed and to whom, despite limitations in both the law and technology (Marwick & boyd, 2014). How do people make the trade-offs involved in using digital platforms? Where do people draw the line between acceptable collection, publication and use of information – and what is creepy or beyond the pale? Another important question is where people perceive that the greatest threats to their privacy comes from: the private sector, government or perhaps their own peers and networks?

In this report, we discuss these interrelated issues of information collection, disclosure and use under the general rubric of privacy. We acknowledge that privacy is a multifaceted and contested concept, long acknowledged to be very difficult to define (Wacks, 1980). It is contextual (Nissenbaum, 2010): it means different things to different people and in different contexts, and can be understood differently across cultures (Altman, 1977). The very way it is understood is changing as we become more enmeshed in digital networks, where our boundaries are no longer entirely ours to individually control (Cohen, 2012; Marwick & boyd, 2014). Privacy is concerned not just with the right to be left alone, or to be protected from intrusion; it is also concerned with controlling our interactions with others (Altman, 1977; ALRC, 2014). In thinking about the rights and responsibilities that users might have in their information relationship with online platforms, privacy is a core organising concept.

Privacy can also be conceived as a *right*, recognised as fundamental at an international level and at least recognised in Australia as a fundamental interest that law should protect (ALRC, 2014). The failure of Australian law to protect privacy has been widely acknowledged – as has government inaction in the face of repeated recommendations to undertake law reform (Daly, 2017). It is important to try to understand what people think and feel about these developments, even as we recognise that their feelings may be heavily determined by context, and may change radically over time. Understanding how people view privacy and the limits of what is acceptable can inform extra-legal developments (such as industry ethical frameworks) and perhaps help us move towards change.

We asked questions across this spectrum. In this chapter, we talk first about general attitudes to privacy, and the private sector context. The related but distinct questions raised by government information processing and surveillance are addressed in Chapter 4. Questions about what expectations employers and employees might have regarding social media use and monitoring are dealt with in our discussion of work in Chapter 5.

3.2 General attitudes towards and understandings of privacy

3.2.1 Are people concerned about privacy?

Australians are concerned about their online privacy. To provide an initial gauge of Australians' feelings about privacy in the digital world, we asked them for their attitudes on two general stereotypes: 'I have nothing to hide' and 'Privacy concerns are exaggerated'. While two-thirds of our respondents believed that they personally had nothing to hide, only a small group (18%) thought that more general debates and public concerns about online privacy were unwarranted. Frequent social media posters (29%) and respondents aged under 40 (25%) were most likely to agree that online privacy concerns were exaggerated. While men (21%), capital city dwellers (21%) and the university educated (21%) were also more likely to agree, the differences were not as substantial. Notably, older people aged over 60 (77%) and those with a high school level of education (74%) were most likely to agree that they had 'nothing to hide'. Those under 40 were the least likely to agree with this proposition (56%).

Table 3.1: 'Concerns about privacy online are exaggerated' (n=1603)

	Agree	Neither	Disagree
Age*			
Under 40	25	32	43
40–59	15	31	54
60+	13	22	65
Gender*			
Male	21	31	48
Female	16	27	57
Location*			
Capital city	21	29	51
Not capital city	15	29	56
Education*			
High school	16	30	53
Technical	16	35	49
University	21	25	54
Posting*			
At least once a day	29	29	41
At least once a week	23	31	46
At least once a month	15	27	58
Less often or never	13	30	57
TOTAL (%)	**18**	**29**	**53**
TOTAL (n)	**294**	**463**	**846**

Table 3.2: 'I have nothing to hide' (n=1603)

	Agree	Neither	Disagree
Age*			
Under 40	56	29	14
40–59	66	24	10
60+	77	17	6
Gender			
Male	64	24	12
Female	66	24	9
Location*			
Capital city	62	26	11
Not capital city	70	21	9
Education*			
High school	74	20	6
Technical	65	27	8
University	60	25	14
Posting			
At least once a day	70	19	11
At least once a week	61	29	11
At least once a month	69	20	11
Less often or never	65	25	10
TOTAL (%)	**65**	**24**	**10**
TOTAL (n)	**1048**	**388**	**167**

3.2.2 What do people do about privacy online (and does it help)?

We also asked respondents whether they took steps to protect their privacy online and whether they felt in control. This is important because where rights to privacy are protected, for the most part the law treats privacy as an individual right (Cohen, 2012). On social media platforms, privacy is given technical effect through access control lists, in which users can determine who can get access to certain information. We included an example of whether they had changed these privacy settings on their most used social media platform (which for the vast majority was Facebook), and whether they feel like they have control over their privacy in the everyday digital context.

Tables 3.3, 3.4 and 3.5 suggest that, on the whole, people do not feel in control of their privacy online, and that taking active steps to protect privacy online does not lead to a feeling of control.

The group most likely to agree that they actively protect their privacy online were the everyday social media posters (75% agreed). These people were also most likely to change their privacy settings (69%) and most likely to feel in control of their privacy (55%). Similarly, people under 40 also changed their settings (67%) and were more likely than the average user to feel that they could control their privacy online (46%). This suggests that frequent public posting is related to feelings of confidence about using platforms regularly, but also to feeling in control of any potential incursions into privacy.

Table 3.3: I actively protect my privacy online (n=1603)

	Agree	Neither	Disagree
Age			
Under 40	67	28	5
40–59	69	26	6
60+	66	29	5
Gender*			
Male	63	30	7
Female	71	25	4
Education*			
High school	65	29	5
Technical	62	31	6
University	71	24	5
Posting*			
At least once a day	75	21	4
At least once a week	66	29	6
At least once a month	63	29	9
Less often or never	65	29	6
TOTAL (%)	**67**	**28**	**5**
TOTAL (n)	**1077**	**441**	**85**

Women (71%) were very likely to agree that they actively protected their privacy online and changed their social media settings (63%), but they felt no more in control of their privacy than men (38%). Taken together with their greater tendency to disagree that concerns about privacy are exaggerated (Table 3.1), this suggests that women generally experience the online world differently.

Table 3.4: Thinking specifically about the social media platform you use most often, have you changed the privacy settings from the original default setting to restrict who can access your profile? (n=1263)

	Yes
Age*	
Under 40	67
40–59	59
60+	51
Gender*	
Male	57
Female	63
Education	
High school	58
Technical	57
University	64

	Yes
Posting*	
At least once a day	69
At least once a week	62
At least once a month	65
Less often or never	52
TOTAL (%)	**61**

These findings are particularly striking in light of the fact that 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 uses. Recent discussions at the policy level, such as Productivity Commission's *Data Availability and Use* report relating to government data sharing, also centre around the idea of giving people more control over their data (Productivity Commission, 2017).

On the other hand, the feeling of a lack of control is not surprising. The privacy features and settings of social media platforms vary widely, from a simple public/private option on Twitter and Instagram to a web of privacy and disclosure settings on Facebook. But, broadly speaking, privacy settings common on social media platforms give users some measure of control over who in their social networks can see what, and what material is exposed to the open internet. Yet these systems are incomplete. While I may limit who can access my posts online, friends with more public accounts end up exposing information about me to a much broader audience. In this networked environment, we are not entirely in control. Further, online platform settings do not allow users to control what the platform itself or its advertisers can do with the information that is collected. As we discuss in the next section, while people are concerned about the actions of fellow users online, they are more concerned about the privacy threat from corporations.

Table 3.5: I feel I can control my privacy online (n=1603)

	Agree	Neither	Disagree
Age*			
Under 40	46	36	18
40-59	35	39	27
60+	32	37	31
Gender			
Male	38	37	25
Female	39	37	25
Education*			
High school	42	37	21
Technical	32	39	28
University	39	36	25
Posting*			
At least once a day	55	32	13
At least once a week	45	36	19
At least once a month	35	36	29
Less often or never	31	42	27
TOTAL (%)	**38**	**37**	**25**
TOTAL (n)	**612**	**595**	**396**

3.2.3 Where does the privacy threat come from?

We asked where our respondents believed the threat to their privacy came from. The answer was primarily 'corporations'. A majority agree that they were concerned about their privacy being violated by corporations (57%), while a substantial number were also concerned about violations by government (47%) and other people (47%). There were very few differences of substance among sub-sets of our respondents in their concern about corporations violating their online privacy, with just the university educated (61%), daily social media posters (61%) and those living in capital cities (60%) slightly more concerned than the average. In terms of other people violating privacy, there were again few substantial differences in the perceptions among sub-groups among our respondents. The main exception was that, again, daily social media posters were mostly likely to be concerned about privacy violations by other people (60%). More detailed information about attitudes towards government is included in Chapter 4.

Table 3.7: I am concerned corporations are violating my privacy online (n=1603)

	Agree	Neither	Disagree
Age			
Under 40	58	32	11
40-59	58	33	9
60+	54	35	11
Gender			
Male	59	31	11
Female	55	35	10
Location*			
Capital city	60	31	9
Not capital city	52	36	12
Education*			
High school	55	35	10
Technical	51	36	13
University	61	30	9
Posting			
At least once a day	61	28	11
At least once a week	55	35	10
At least once a month	60	32	8
Less often or never	59	32	10
TOTAL (%)	**57**	**33**	**10**
TOTAL (n)	**910**	**527**	**166**

On social media, it is possible – and common – for people to upload or tag photos of other people, making information public even where a person has strict privacy settings for their own profile. We focused on this specific example of when privacy might be breached by other

3.3 Comparing European Union and Australian responses to data collection and analytics

In a world of rapidly transforming technology and commercial practice around the collection and use of ever-larger data sets and increasingly advanced data analytics, we might expect to see some response in the legal and regulatory sphere.

The European Union (EU) response has been proactive. European law has long recognised the fundamental right to privacy and to data protection.[1] The EU's new General Data Protection Regulation (GDPR) (European Union, 2016) takes effect in May 2018.[2] 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 [European Union] Member States' (Recital 3). The GDPR includes new rights: the right to be forgotten (Article 17) and the right to data portability (Article 20). It also addresses data profiling, distinguishing between common profiling (analysing or predicting aspects of a natural person's life) and high-risk profiling (where the profiling produces legal effects concerning a person or significantly affects a person). More stringent rules apply to the latter, and could impact activities such as using data analytics for price discrimination (Steppe, 2017). The European Parliament has also been proactive in responding to increasing automation, with a Resolution from February 2017 on Civil Law Rules on Robotics (Daly, 2017). In June 2017, the UK House of Lords established a Select Committee on Artificial Intelligence to consider the economic, ethical and social implications of advances in artificial intelligence, and to make recommendations.

By contrast, Australia's law-makers have been slow to respond (Daly, 2017). Australian privacy law is the result of both legislation and the common law. There is no right to privacy enshrined in the Constitution and, unlike many other liberal democracies, Australia lacks a constitutional or statutory Bill of Rights at the Commonwealth level. 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. This does not provide an enforceable right to privacy. The *Privacy Act* includes thirteen 'Australian Privacy Principles' that broadly impose obligations on organisations 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. Australians, however, have no direct right to sue for a breach – only rights to complain, first to the organisation involved or, if there is no satisfactory response, to the Office of the Australian Information Commissioner.

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, 2017). 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, 2017).

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 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.

For now, Australians' hope of some data protection may be indirect. The GDPR has some global effect – compliance obligations for international organisations or businesses based outside the European Union that have an establishment in the EU, that offer goods and services in the EU, or that monitors or processes the behaviour of individuals in the EU.

people to see how our respondents understood this. A relatively innocuous and frequently occurring activity of sharing a non-intimate photograph online without permission was considered a breach of privacy by the vast majority of our respondents (82%), although those under 40 (77%) were slightly less likely to be concerned by this.

Table 3.8: I am concerned other people are violating my privacy online (n=1603)

	Agree	Neither	Disagree
Age			
Under 40	49	33	17
40-59	48	38	15
60+	43	37	20
Gender			
Male	47	36	18
Female	48	36	16
Education			
High school	48	34	18
Technical	44	36	20
University	49	37	15
Posting*			
At least once a day	60	24	16
At least once a week	44	40	16
At least once a month	47	31	23
Less often or never	46	38	15
TOTAL (%)	**47**	**36**	**17**
TOTAL (n)	**756**	**573**	**274**

Table 3.9: It is a breach of privacy if someone in my social network publishes online a photo of me without my permission

	Breach	Not breach
Age*		
Under 40	77	23
40-59	84	16
60+	87	13
Gender*		
Male	79	21
Female	85	15
Education		
High school	84	16
Technical	81	19
University	81	19
Posting*		
At least once a day	83	17
At least once a week	71	29
At least once a month	82	18
Less often or never	86	14
TOTAL (%)	**82**	**18**
TOTAL (n)	**1248**	**271**

3.4 Data analytics, targeting and discrimination

How information is *used* is to shape our online interactions is a question of growing public discussion. Data analytics, the use of machine learning and other related technologies can affect – and harm – individuals or broader societal interests even where no personal information is ever disclosed. These developments give rise to broader concerns around maintenance of consumer trust, fairness of opportunities and outcomes, and avoiding biases in decision-making and skewing of communications that can result from the application of data analytics (Leonard, 2017).

In commerce, highly targeted advertising, price discrimination and issues around automated processing of job applications have all attracted attention, giving rise to suggestions that new legal and ethical frameworks are needed (Yeung, 2017).

We asked respondents whether they wanted to know more about what social media platforms and other online companies do with the data generated by and about them. In particular, we asked how important it was to them to access reports on the internet user profiles constructed about them. Large majorities of respondents believed it was either very important or important to be able to access reports of:

- what third-party companies do with your personal information – 78%
- the list of third-party companies that can access your profile – 75%
- records of what you have done on social media – 55%
- records of what you have bought online – 54%.

People were not concerned so much about what information is collected or held; rather, they were far more interested in what corporate platforms, and others like advertisers, *do* with the information. This is reinforced in Table 3.10, which shows that a large majority of respondents (78%) wanted to know what social media companies did with their personal data. Again, everyday social media posters (86%) were the most likely to agree. Interestingly, those aged under 40 (72%) were significantly less likely to agree that they wanted to know about this form of data use.

Attitudes towards use of data analytics, targeting and personalisation are hard to address through a survey, because people's attitudes to these issues are nuanced and context-dependent. Our online focus group was used to explore these questions further. In this way, the study was able to test how participants responded to different scenarios in which their data was collected, analysed and subsequently used by private companies. The questions started at a very general level ('How do you broadly feel about internet companies using the data you share with them (such as emails, social media

activity) for marketing purposes, and why') and became more specific.

Table 3.10: I want to know what social media companies do with the information they collect, share, keep and use about me

	Agree	Neither	Disagree
Age*			
Under 40	72	23	5
40-59	81	15	4
60+	82	14	4
Gender*			
Male	73	22	5
Female	82	14	4
Location*			
Capital city	79	17	3
Not capital city	75	19	6
Education*			
High school	77	18	6
Technical	74	21	5
University	81	16	3
Posting*			
At least once a day	86	12	2
At least once a week	76	20	4
At least once a month	77	17	6
Less often or never	80	17	4
TOTAL (%)	**78**	**18**	**4**
TOTAL (n)	**1248**	**286**	**69**

The first scenario related to companies using collected data to target advertising to them. Responses to this question fell broadly into two camps. Some people said that it 'feels like someone is watching', describing the feeling as 'creepy' and a 'violation of privacy':

> *I hate the idea of targeting ads … the simple fact is Gmail is effectively selling out my private details [which] may seem harmless, but where does it end?*

Other members of the focus group thought that targeted advertising was harmless – perhaps even convenient: 'I don't mind, as it's clearly something or a particular service I will go search for in my own time.' Given the scenario of Gmail targeting ads for holiday packages at you because you wrote 'I need a holiday' in a recent email, one panellist commented that 'I don't have to surf the web, it's almost like it's being done for me'. Another described targeted advertising as 'just an evolution of advertising'. Another was explicit about the trade-off:

> *I also find it a bit invasive but the upside is being able to grab a good deal.*

Reinforcing the importance of context, as well as the importance of personal responsibility, one participant highlighted that there might be different expectations of privacy between online platforms:

> *If you are going to post 'I need a holiday' on a giant billion dollar social aggregate like Facebook, I would be very surprised if I didn't start getting targeted ads. So far as looking for information in something like my emails? That is a breach of privacy and would lead to discontinuing my affiliation with the service.*

Another documented use of data analytics in commerce is to offer different prices to different consumers (White House Executive Office, 2015). Faced with a scenario of differential pricing offering by companies on internet platforms, the views of our panellists were mixed.

In the case of different prices being advertised based on a user's gender for a service (such as car mechanical servicing), most people felt uncomfortable, citing notions of gender inequity and the fact that this practice fed into such discriminatory practices. However, in a different scenario – such as a particular designer clothing company choosing not to show ads to consumers who lived in lower socioeconomic areas – responses were more divided, with some believing everyone should see the same thing on the internet, regardless of where they lived, while many didn't see this practice as problematic, believing it was simply 'smart advertising' or 'just marketing'.

More recently, the lack of transparency around highly targeted political advertising on platforms like Facebook has attracted sufficient international attention to prod some response from social media companies, with Facebook, Twitter and Google all announcing new transparency measures around political advertising in October 2017 (e.g. Facebook, 2017). Note that our online panel discussion was conducted in August 2017, before the recent flurry of news coverage and activity.

There was a clear consensus among participants when it came to the matter of targeted political advertising on social media platforms. Most agreed that content targeting for political purposes should be treated differently from targeting for marketing. For example, if a political party were to pay Facebook to boost a negative opinion article about a rival party to Facebook users who live in marginal seats, this scenario was seen as crossing a line in terms of social media use, even by those who expressed little interest in politics or little trust in politicians:

> *[P]ersonally I really don't care about politics but I just think it's wrong to use social media for that purpose.*

> *Social media shouldn't be able to bias one party due to being paid by the other, it's downright wrong and a complete sham.*

Some participants were less concerned about this type of data analytics in social media use, or were prepared to simply ignore it even if they encountered such targeted political advertising themselves. There is nothing new, after all, about 'biased' political advertising.

Endnotes

1 Data protection is enshrined in the Treaty on the Functioning of the European Union (Article 16), which provides that: 'Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.' According to the Treaty, everybody has the right to the protection of personal data concerning them. The fundamental right to the protection of personal data is explicitly recognised also in Article 8 of the Charter of Fundamental Rights of the European Union. The right to privacy (more generally) is recognised in Article 8.

2 Note that in the EU, a regulation is more powerful than a Directive. As a regulation, the GDPR is not to be transposed into national law but forms an automatic part of it.

Chapter 4

Government data matching and surveillance

Core findings

- Nearly half of our respondents were concerned about government violating their privacy (47%).
- A majority were opposed to government programs for phone companies and internet service providers to keep metadata on phone calls and web use. Some 79% of respondents considered retention of information about phone calls to be a privacy breach. A majority (58%) were also opposed to a policy for government-mandated retention of information about internet communications.
- But a change in frame altered these numbers. When asked whether they favoured *law enforcement and security agencies* being able to access metadata, the number in favour jumped to 42% (47% opposed). However, when framed as an *anti-terrorism* measure, government data-gathering about the internet was supported by a majority of respondents (57%), while only 31% opposed a program described in this way.
- Our findings highlight the critical importance of the framing of questions when assessing public support for data collection and sharing, and interpreting survey results.
- Respondents' attitudes towards both government collection of communications data, and government data matching programs, varied significantly depending on political identification. Respondents who identified with the Coalition were significantly more likely to support programs; identification with the Greens made a respondent more likely to oppose such programs.
- There was considerable ambivalence among the survey participants towards online government data matching programs. We found that 42% were in favour and 45% were opposed to a program that tracked citizen use of public services and benefits. The members of our online focus group were also sharply divided on a range of data matching scenarios put to them.

4.1 Legal and policy issues in government collection and use of data

Governments are keen to use the capacities of data analytics to better plan and efficiently target government services and spending, to enable more effective law enforcement and to boost local innovation and the development of commercial services based on government data (such as real-time, third-party public transport apps like TripView and Moovit).

But data matching and use of data analytics by government, or by government sharing data with the private sector, raise distinct questions about the power of the state and the nature and sheer scale of the data governments possess. Individuals in general have less choice about providing personal information to governments. They also typically see less immediate, personal benefit from doing so (Productivity Commission, 2017).

The Australian Productivity Commission's March 2017 *Data Availability and Use* report examined opportunities and issues arising from increasing access to, and availability and linking of, data between government agencies, as well as expanding sharing of data between the public sector, private sector, researchers and academics, and the broader community. The Commission's report constitutes the first attempt to comprehensively review the use of data within government and across sectors in Australia.

The Commission noted that Australia's legal and policy frameworks for collection, storage and use of public- and private-sector data are ad hoc and not contemporary, and that, as a result, Australia is not participating in developments in the use of data or benefiting from data-driven services and efficiencies. The Productivity Commission called for fundamental, systematic change in the ways governments, businesses *and* individuals

handle data (Productivity Commission, 2017, p. 12). The Commission's framework would both increase potential for data sharing and release, *and* give Australians more control over their digital data.

The Productivity Commission is not alone in its views. The Australian Computer Society recently released a Technical White Paper on Data Sharing Frameworks with a view to supporting the development of smart services and a better understanding of a wider network of individuals and (government and private) services and service providers (Australian Computer Society, 2017).

The ACS White Paper, like the Productivity Commission report, highlighted the potential benefits of data-sharing within and across sectors. The White Paper also highlights the fundamental challenges that lie in the interface between technical needs for precise concepts and definitions, and legal and ethical frameworks that tend to be nuanced and based on fuzzy standards like reasonableness. The White Paper supports the need to develop clear and concise legal, policy and ethical frameworks to enable data-sharing while still protecting individuals' rights, including their privacy – as well as to confront the difficult questions around data use: *Just because we can, should we?*

At the same time that this high-level policy discussion around the potential of government and private sector data-sharing is occurring, Australia has seen some high-profile debates related to government collection, storage and use of data and data matching, especially in the law enforcement context. One significant policy shift in recent times has been the introduction of a legal obligation on telecommunications providers to store *metadata* – data about individuals' use of internet and phone services (such as what numbers people have called, when and for how long) without including the content of communications (Leonard, 2016). These developments are discussed further below.

Another public debate arose when the government undertook large-scale matching of tax data with information about government benefits – and used that information to send debt notices to past welfare recipients. Both debates are discussed further below, and both provided some specific questions for consideration in our study.

The Productivity Commission and the ACS White Paper both emphasise the importance of trust and the social licence for the continued collection and use of data. In this context, understanding public support (or lack of it) for the use and collection of data, and the conditions people place on their support, are important if we are to respond to calls to develop new legal, policy and ethical frameworks to successfully navigate this rapidly changing environment.

4.2 General attitudes towards government and government-mandated data collection

In Chapter 3, we reported survey data on whether people were concerned about corporations, other people or governments violating their privacy. Chapter 3 reported that while a majority agreed that they were concerned about their privacy being violated by corporations (57%), a substantial number remained concerned about violations by government (47%).

Table 4.1 breaks down the data relating to respondents' concerns about violations by government (for equivalent tables regarding violations by corporations and individuals, see Chapter 3). In terms of governments and other people violating privacy, there were few differences between sub-groups. The most substantial differences in view are related to partisanship. Green voters were most likely to be concerned about governments violating their privacy (54%) and Coalition voters were the least likely to be concerned (38%). The group of people not concerned about governments violating their privacy is small overall (16%) with a large group (37%) not prepared to either agree or disagree with the suggestion that they had concerns.

Table 4.1: I am concerned governments are violating my privacy online (n=1603)

	Agree	Neither	Disagree
Age			
Under 40	50	35	15
40–59	45	41	15
60+	44	37	19
Gender*			
Male	50	35	15
Female	43	40	17
Education			
High school	47	35	18
Technical	43	41	16
University	48	37	15
Posting			
At least once a day	56	28	16
At least once a week	47	38	15
At least once a month	48	37	16
Less often or never	44	40	16
Party*			
Labor	50	37	14
LNP	38	40	22
Greens	54	31	15
Other	50	33	17
None/DK	48	40	12
TOTAL (%)	**47**	**37**	**16**
TOTAL (n)	**747**	**601**	**255**

4.3 Australia's shift to require retention of data about communications (metadata)

The Commonwealth Government introduced wide-ranging and mandatory metadata retention provisions under the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth). The obligations under this Act came into full effect on 14 April 2017, and required telecommunications service providers to retain specified metadata for at least two years (Leonard, 2016).

Metadata is complex to define, but can broadly be characterised as the background technical information generated by an electronic communication, excluding the content of the communication itself. Metadata encompasses information including when, where, how and with whom a communication occurs via phone or the internet, as well as information about internet usage, uploads and downloads, email addresses and call-related features used on a mobile phone.

What people say in an email or on the phone is, of course, informative, but even without a transcript, information about the email or call can be revealing. Who are you talking to? When and where were you when you had the conversation? A series of conversations with a cancer clinic, for example, could reveal that a person has cancer. Repeated conversations with a political organisation like Getup! could reveal political orientations, especially if coincident with known advocacy campaigns. Over time, metadata can create insights into a person's individual patterns of behaviour, including their geographical location, associations and interactions with other people in Australia and overseas, as well as information that may be gleaned about their daily routine, interests, education, political and religious opinions, medical conditions and personal lives.

Prior to the introduction of the 2015 Act, metadata was routinely accessed for law enforcement and intelligence purposes, but retention practices varied significantly. Debate surrounding the passage of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth)* was framed by both the Coalition government and the Labor Opposition as a matter of national security, and as key to counter-terrorism efforts. Senator Mitch Fifield, then Manager of Government Business in the Senate and Assistant Minister for Social Services, stated in the Second Reading Speech that the passage of the Bill was crucial to 'prevent the capabilities of Australia's law enforcement and national security agencies being further degraded' because 'access to metadata plays a central role in almost every counterterrorism, counterespionage, cybersecurity and organised crime investigation' (Commonwealth of Australia, Senate, 24 March 2015).

The potential set of persons who can seek access to metadata is, however, potentially broader than just Australia's national security agencies: it currently includes both the Australian Securities and Investment Commission and the Australian Competition and Consumer Commission, as well as the Australian Border Force. To date, a much longer list of organisations (like local councils) who applied for access have not been added to the approved list, and metadata is not available to civil litigants (Australian Government, 2017).

4.4 Government-mandated retention of communications-related data

We sought to investigate respondents' attitudes towards the retention of metadata through a series of questions, with more or less specificity about the purpose of the collection or use.

Table 4.2 sets out responses when we asked *generally* whether respondents considered *phone* companies should be required to keep information about who was called and when there was a breach of privacy, without specifying the purpose of collection.

We found that 79% of respondents considered this to be a breach of their privacy. The high school educated (84%), Greens identifiers (84%) and women (83%) were most likely to agree that this was a privacy breach, while Coalition identifiers were significantly less likely to see it as a breach (73%) – although that figure still represents a substantial majority.

We also asked about *internet* communications, again without specifying any particular purpose for the requirement for internet service providers to keep metadata. When the question was framed in this way, only 31% (overall) were in favour of a general requirement for internet service providers to keep metadata, with a majority (58%) opposed to this policy. Those most likely to be in favour included Coalition identifiers (46%), everyday social media posters (39%) and the university educated (35%). Those most likely to be opposed were Greens identifiers (65%).

Table 4.2: Is it a breach of privacy if the government requires my phone company to keep information about who I call and when?

	Breach	Not breach
Age		
Under 40	79	21
40–59	81	19
60+	78	22
Gender*		
Male	76	24
Female	83	17
Education*		
High school	84	16
Technical	76	24
University	78	22
Posting		
At least once a day	80	20
At least once a week	79	21
At least once a month	83	17
Less often or never	80	20
Party*		
Labor	82	18
LNP	73	27
Greens	84	16
Other	76	24
None/DK	83	17
TOTAL (%)	**79**	**21**
TOTAL (n)	**1192**	**309**

Table 4.3: Do you favour or oppose the government requiring internet service providers to store information about who you contact, when, and what websites you visit (n=1603)

	Favour	Unsure	Oppose
Age*			
Under 40	30	14	56
40–59	30	12	58
60+	34	6	60
Gender			
Male	32	11	57
Female	30	12	58
Education*			
High school	27	12	61
Technical	29	13	57
University	35	9	56
Posting*			
At least once a day	39	8	53
At least once a week	35	9	56
At least once a month	29	10	61
Less often or never	24	14	62
Party*			
Labor	30	8	62
LNP	46	7	47
Greens	24	10	65
Other	30	8	62
None/DK	22	20	59
TOTAL (%)	**31**	**11**	**58**
TOTAL (n)	**500**	**179**	**924**

When a law enforcement or national security angle was added to the question, however, support rose. Thus, when asked whether they favour law enforcement and security agencies being able to access metadata, the number in favour jumped up to 42%, and 47% opposed. Coalition party identifiers (54%) remain the groups most likely to favour this kind of access. Green party identifiers were the only group to significantly oppose this policy (57%).

Table 4.4: Do you favour or oppose law enforcement and security agencies being able to access information about who you contact, when, and what websites you visit (n=1603)

	Favour	Unsure	Oppose
Age*			
Under 40	40	14	45
40–59	41	12	47
60+	46	5	50
Gender			
Male	42	11	48
Female	42	12	46
Education			
High school	39	13	48
Technical	41	13	46
University	44	9	47
Posting*			
At least once a day	49	7	43
At least once a week	46	8	46
At least once a month	39	12	49
Less often or never	36	17	48
Party*			
Labor	42	9	49
LNP	54	6	40
Greens	35	7	57
Other	41	9	50
None/DK	34	20	46
TOTAL (%)	**42**	**11**	**47**
TOTAL (n)	**672**	**179**	**752**

The responses shifted even further once the question was framed in terms of anti-terrorism efforts. We asked about a government program to collect communications of nearly all internet users as part of anti-terrorism policies. Here the majority of respondents (57%) are in favour while only 31% oppose this kind of program. Interestingly, these results echo Roy Morgan survey results regarding the Australian government's new 'anti-terror' laws requiring state governments to provide licences for mass facial-recognition technology. A special Roy Morgan Snap SMS Survey was conducted over the weekend of 7–9 October 2017, with a cross-section of 1486 Australians aged 18+. In that survey, respondents were asked, 'Under anti-terror measures State Governments will provide driver licence photos for mass facial recognition technology. Does this concern you?' A total of 67.5% of survey respondents were not concerned, compared with 32.5% who expressed concern.

Those most likely to be in favour of this kind of program included Coalition party identifiers (69%), those aged over 60 (64%), everyday social media posters (62%) and the high school educated (62%). Greens identifiers (47%) were the only group significantly more likely to oppose this policy.

Clearly, there is salience for metadata data collection and surveillance when it is framed in security and anti-terrorism terms. Privacy is important to Australians, but can be forsaken or traded off against security fears.

Table 4.5: Do you favour or oppose a government program to collect communications of nearly all internet users as part of anti-terrorism efforts (n=1603)

	Favour	Unsure	Oppose
Age*			
Under 40	52	16	32
40–59	56	12	31
60+	64	6	29
Gender*			
Male	54	11	35
Female	59	13	28
Education*			
High school	62	11	27
Technical	50	17	33
University	57	10	33
Posting*			
At least once a day	62	8	30
At least once a week	57	10	33
At least once a month	57	11	33
Less often or never	53	18	30
Party*			
Labor	56	10	34
LNP	69	7	24
Greens	41	12	47
Other	57	9	34
None / DK	51	21	27
TOTAL (%)	**57**	**12**	**31**
TOTAL (n)	**909**	**195**	**499**

4.5 Government data matching

Data matching has been described broadly as the large-scale comparison of records or files collected or held regarding an already identified individual for different purposes, with a view to detecting matters of interest. Data matching involves bringing together disparate pieces of information from different sources, and compiling and comparing it. Data matching is distinct from data linking, which involves linking identified databases with anonymous databases to re-identify or de-anonymise the previously anonymous data by linking and examining the digital fingerprint.

In the Australian context, data matching is generally carried out by Commonwealth, state and territory government agencies with large troves of data, such as the Australian Taxation Office (ATO), the Department of Human Services, the Department of Veterans' Affairs, the Department of Immigration and Border Protection and the relevant health departments. The ATO also engages in data matching with non-government, third-party sources to identify fraud, including banks and financial institutions, online selling sites like eBay, and those facilitating the 'sharing economy', such as Uber, Airtasker and Airbnb.

Until recently, there was limited ability to match the data held by various government entities, and little appetite to do so. However, in recent years government interest in data matching for the purposes of planning and targeting services has increased considerably.

As Table 4.6 shows, there is considerable polarisation among the survey participants towards an online government data matching program that tracks citizens' use of public services and benefits. We found that 42% were in favour and 45% were opposed to this kind of program (with only a small proportion unsure, compared with the larger ambivalent or unsure groups we saw in the previous chapter).

Those most likely to be in favour included Coalition identifiers (54%), university educated respondents (48%) and men (46%); those most likely to be opposed included those who identified with a non-major party (53%) and respondents over 60 (49%).

In keeping with the survey responses above, respondents in the online focus group were strongly divided about government data sharing and data monitoring.

Table 4.6: Do you favour or oppose a government program that tracks your use of public services and benefits (n=1603)

	Favour	Unsure	Oppose
Age*			
Under 40	42	18	41
40–59	41	13	46
60+	45	6	49
Gender*			
Male	46	12	42
Female	39	14	47
Education*			
High school	38	13	48
Technical	37	16	47
University	48	11	41
Posting*			
At least once a day	46	8	46
At least once a week	42	12	46
At least once a month	42	14	43
Less often or never	37	18	45
Party*			
Labor	43	10	46
LNP	54	8	38
Greens	39	12	48
Other	40	7	53
None/DK	33	22	45
TOTAL (%)	**42**	**13**	**45**
TOTAL (n)	**677**	**207**	**719**

For some, there is a clear benefit – for example, in government departments sharing citizen data among themselves for the purposes of improving service delivery. We asked participants, 'How do you broadly feel about government departments sharing your personal data (including things like tax, social security, criminal history and medical records) between each other for service delivery?' For example, participants stated:

> *I am happy for the government departments to share information. I wish my medical records could be all stored in one place; that way when I see a doctor from another practice all the information would be there and I wouldn't have to explain my history over and over.*

> *Broadly I'm okay with this. It would make some services easier to deliver and administer such as combining a car licence with a firearms licence.*

There were conditions for such support, with participants commenting on the need for 'BIG safeguards' and accountability for abuse. Some made their support conditional on data sharing being confined to within-government sharing. Two participants said they would only support sharing if they had given permission.

One hypothetical scenario given to respondents was that of the tax office collating data in order to assist with individual tax returns. Half of the participants believed this was a good idea, given its likelihood to ensure they received all of their entitlements, as well as the chance to reduce tax evasion or fraud. However, the other half were not convinced, either because they believed such data sharing should only take place under certain conditions – such as where individual permission was granted, or there was anonymity of data, or because it was seen as just another means by which the government could surveil and monitor citizens.

We also asked the members of the online focus group for their reaction if schools could share a student's attendance data and personal information with community police in order to identify and intervene with students in need of support. Here, too, responses were polarised. Half thought this was a good idea, based on its ability to improve social outcomes and promote the public good (whether framed as 'helping children in need' or 'helping policy catch children who break the law'). But the other half were strongly against such a proposal, seeing it as a clear instance of government over-reach into citizens' lives, and as adding further surveillance in a society where there is already enough government monitoring:

> *The example sounds good in theory; however, it can then easily be expanded into a 1984 scenario.*

Another scenario we put to the online focus group imagined the linking of health and travel data in order to notify citizens who had been in the same location as a person with a contagious disease such a measles. Again, half the respondents expressed concern about the proposal, describing it as 'Big Brotherish' or 'creepy'. But half were in favour ('I think if it's the government it's totally okay', or 'great idea'). Some who were supportive in principle, however, expressed a higher level of caution given the way this scenario seemed more interventionist; some said they would only feel comfortable if the data were anonymised (although this would not be possible in the scenario given).

4.6 Centrelink's data matching program and #notmydebt

The complex issues around data matching are exemplified by the #NotMyDebt social media campaign and subsequent parliamentary inquiry. This story started to attract attention online in December 2016 and January 2017.

Data matching has been carried out between Centrelink and the Australian Taxation Office (ATO) for over approximately 20 years, with the aim of reducing fraudulent over-payments. However, this controversy arose in relation to an automated data matching procedure being used to compare income during the financial years from 2010–11 to 2012–13. People started to receive letters stating that they owed Centrelink significant debts as a result of over-payment of government entitlements.

It was subsequently revealed that Centrelink was utilising an 'Online Compliance Intervention' computer program that issued letters based on automated data matching procedures between Centrelink and the ATO. When the program identified a discrepancy between the annual total income an individual declared to the ATO and Centrelink's fortnightly payment records, a letter was automatically generated and sent to the recipient.

The algorithm presumed that income had been earned at a constant level throughout the financial year, and used this averaged income to estimate fortnightly Centrelink entitlements. The algorithm did not take into account fluctuations in income throughout the financial year, such as those working on a casual or seasonal basis. Moreover, the process was altered so that, instead of a Centrelink official liaising with the recipients' employer to confirm income, this responsibility was shifted to the recipient.

The automated and crude nature of the data matching algorithm, as well as the generation of letters demanding repayment of purported debt, resulted in the program being described colloquially as a 'robo-debt'. The Senate Community Affairs References Committee reported that between November 2016 and March 2017, at least 200,000 people were impacted by this program.

In February 2017, the Senate Community Affairs References Committee commenced an inquiry into these events. The inquiry's report, *Design, Scope, Cost–Benefit Analysis, Contracts Awarded and Implementation Associated with the Better Management of the Social Welfare System Initiative*, was published in June 2017 (Senate Community Affairs References Committee, 2017). The Committee received 156 submissions and more than 1400 emails from individuals, with significant emphasis being placed on the personal and emotional impact of the program on vulnerable welfare recipients. The final report was very critical of the program, recommending that the Online Compliance Intervention (OCI) program should be put on hold until all procedural fairness flaws (and the Committee's own recommendations) were addressed (Senate Community Affairs References Committee, 2017). The government, however, rejected this recommendation.

Chapter 5

Work

Core findings

- Digital privacy at work matters. Most Australians do not think employers should look at their employees' social media pages. While 37% agreed that it was acceptable for either prospective or current employers to look at *public* social media posts, only 20% agreed that it was acceptable for either current or prospective employers to look at *private* posts.
- High school educated people, those not working in professional/skilled work and respondents over 40 were most concerned about employers accessing their social media posts.
- Only 16% of people agreed that using social media was an important part of their job, but most of their workplaces (72%) had a policy about using social media while at work. Most workplaces seemed to recognise the everyday ubiquity of social media use and were attempting to govern it, though only 46% of respondents said their workplace had a policy on *what* they posted online.
- In this terrain of unclear directions over social media at work and employers' rights to access posts, our online discussion groups reinforced that privacy boundaries were important, but also that employees needed to use their own 'common sense'.
- The encroachment of some new policy agendas, such as that seen in the case study of the Public Service Commission, needs to better reflect citizens' desires for digital privacy at and from work.
- The app-driven, online gig economy presents a new space for digital rights analysis. Most respondents have heard of, but not used, a platform such as Uber, Airtasker or Deliveroo, and use is skewed towards those under 40 and the university educated.
- Australians see gig work as providing workers with more flexibility, but at the same time a majority of people are also concerned about the financial insecurity of this kind of work. Over 60% of respondents believed that these new forms of work needed new government regulations. Yet, as shown in the case study, institutionalising fairer regulations is fraught.

5.1 Digital privacy at work

The social media activity of citizens has presented a dilemma in the employment context. Use of social media has become integral to many workplaces; at the same time, our personal lives are permeated by the use of social media platforms:

> Where other technological developments such as email, mobile phones, laptop computers, and remote-access intranet facilities had already diffused and continue to dim the physical and psychological boundaries between employees' public and private lives … social media developments arguably have intensified this penetration of employers into the personal lives of workers. (Thornthwaite, 2013, p. 167)

It is further noted that 'social media provides an avenue potentially to expand the scope of employees' obligations in their personal time, without a reciprocal growth in employers' responsibilities' (Thornthwaite, 2013, p. 164).

In their engagements online, when do individuals cease to act in their private capacity and take on the obligations of an employee? Is there such a thing as digital privacy at work? What is the appropriate balance be found between employer rights to protect the reputation of their brand and employee rights to speak freely online? Where, in the digital realm, does an employee's responsibility to their employer end? And to what extent should employers be allowed to monitor the social media communications of their employees? This is an area of employment relations that is still in its infancy.

In Australia, currently there is no constitutional, statutory, tort or common law 'right to privacy' that would protect

employees from what evidence suggests is 'a growing intrusion of employer control in [employees'] private lives' (Thornthwaite, 2013, p. 5). As discussed in earlier chapters, the concept of privacy remains contested. Social media use at work throws into the mix the issue of digital privacy. Social media use is increasingly used in disciplinary and dismissal decisions of employers, evidenced by the increasing number of unfair dismissal cases being brought before industrial tribunals such as the Australian Industrial Relations Commission and Fair Work Commission. Yet the key issues being raised about the extent to which employers can regulate what employees do online in their private capacity remain largely unresolved (Thornthwaite, 2013, p. 184).

In the survey, we asked respondents a series of questions about their use of social media at work and their perception of their rights to digital privacy while at work. We are interested in the idea of digital privacy and how it effects all areas of our lives. An initial question we asked was whether respondents believed that it was a breach of privacy if future or prospective employers looked at their public social media profile. This would presumably include a public Twitter, LinkedIn or Instagram account, but not a Facebook or Snapchat account, as they are often more private and a prospective employer is unlikely to be part of an existing network of family and 'friends'. This question with regard to prospective employers draws upon the observed phenomenon in relation to employers' use of social media as part of the 'profiling' of potential recruits (McDonald and Thompson, 2016).

Table 5.1 shows that there is some ambivalence about what constitutes a breach of digital privacy. In general, half our respondents considered that a prospective employer looking at a public social media profile constituted a breach, while half did not. There were no differences here by age or gender. There was a difference, however: those who were high school educated and those who lived in capital cities felt it was more likely to be a breach.

This trend is reinforced in the responses to the next question (Table 5.2), where those respondents who were high school educated were less likely than university-educated respondents to see that social media was relevant to their job in any way. Frequent, daily social media posters were the group *most likely* to consider this a breach of privacy. Thus frequent and active users of social media were more committed to the idea that there was public social media posting and private posting, and felt that the context for digital privacy mattered.

Table 5.1: Is it a breach of privacy if a prospective employer looks at my *public* social media profile?

	Yes, a breach
Age	
Under 40	48
40–59	49
60+	51
Gender	
Male	49
Female	50
Location*	
Capital city	52
Not capital city	46
Education*	
High school	55
Technical	47
University	47

	Yes, a breach
Posting*	
At least once a day	64
At least once a week	45
At least once a month	46
Less often or never	47
TOTAL (%)	**50**
TOTAL (n)	**746**

Table 5.2 shows that only 16% of respondents agreed that social media was an important part of their work and those who agreed that social media was helpful for their work were skewed towards those under 40, men, professional workers, and frequent social media posters. This suggests that there may be a divide between public social media that is useful for paid work, versus the experience of most participants where social media use is about sociality or information gathering with personalised networks of family and friends.

In this context of a blurring between the use of social media for and in our public and private lives, we also asked four questions (Tables 5.3, 5.4, 5.5, 5.6) about whether it was acceptable for both current and prospective employers to look at what people post on social media. Overall, just over a third of respondents (37%) agreed that it was acceptable for either prospective or current employers to look at public social media posts, while only 20% agreed that it was okay for either current or prospective employers to look at private posts. While there is a certain amount of ambivalence across the sample, with 20–25% selecting 'neither', it does suggest that there are few people who really agree that all social media are now public, and thus it is perfectly acceptable for employers to access employees' social media profiles and postings. This ambivalence, which often depends on an assertion of common-sense circumstances, is still underpinned by a concern for digital privacy and is reinforced in our qualitative online discussion groups, discussed below.

Table 5.2: 'Social media is important for helping me do my work or job'

	Agree	Neither	Disagree
Age*			
Under 40	27	33	40
40–59	15	27	58
60+	2	35	63
Gender*			
Male	19	32	49
Female	13	31	56
Education			
High school	13	33	54
Technical	14	30	55
University	19	30	50
Posting*			
At least once a day	31	29	40
At least once a week	25	35	41
At least once a month	18	40	42
Less often or never	9	27	64
Profession			
Professional or skilled	24	26	50
Not professional or skilled	17	29	55
TOTAL (%)	**16**	**31**	**53**
TOTAL (n)	**130**	**249**	**422**

Table 5.3: 'It is acceptable for current employers to look at your public social media posts'

	Agree	Neither	Disagree
Age*			
Under 40	43	31	26
40–59	34	28	38
60+	32	27	41
Gender			
Male	39	28	33
Female	35	29	36
Education*			
High school	31	28	41
Technical	34	32	33
University	43	27	31
Posting			
At least once a day	41	24	35
At least once a week	43	27	30
At least once a month	38	26	37
Less often or never	32	32	36
Profession			
Professional or skilled	44	26	29
Not professional or skilled	33	32	35
TOTAL (%)	**37**	**29**	**34**
TOTAL (n)	**295**	**230**	**276**

Table 5.4: 'It is acceptable for current employers to look at your private social media posts'

	Agree	Neither	Disagree
Age*			
Under 40	26	30	45
40–59	16	25	59
60+	18	21	62
Gender			
Male	22	24	54
Female	18	27	55
Education			
High school	18	26	56
Technical	19	30	51
University	22	23	55
Posting*			
At least once a day	28	19	53
At least once a week	23	27	50
At least once a month	16	25	59
Less often or never	14	29	58
Profession			
Professional or skilled	24	25	51
Not professional or skilled	19	27	55
TOTAL (%)	**20**	**25**	**55**
TOTAL (n)	**159**	**204**	**438**

We did identify variation in agreement on whether it is acceptable for employers to access social media posts. Those under 40 were more likely than those over 40 to agree that current and prospective employers could look at public posts, and that current employers could look at private posts. A majority across all age groups disagreed with prospective employers looking at private posts. Interestingly, frequent posters were also more likely than infrequent posters to agree that it was acceptable for both current and prospective employees to look at social media posts. While most frequent posters still disagreed with accessing private posts, those who used social media a lot were slightly more likely to be open to the idea that everything is more public now, but this was also likely to be highly correlated with youth. Lastly, university educated respondents thought it was more acceptable for both current and prospective employers to look at public social media posts of employees. This attitude potentially comes from the point of view of employers as we also observe a difference between what professionals/highly skilled think versus those not in professional or skilled work. Correspondingly, those who had only completed high school were consistently the group to be least likely to agree that it was acceptable for any employer to look at public or private social media posts – potentially these are the least powerful employees, who are most subject to this kind of infringement on their digital privacy.

Table 5.5: 'It is acceptable for prospective employers to look at your public social media posts'

	Agree	Neither	Disagree
Age*			
Under 40	41	31	27
40–59	35	28	38
60+	36	25	39
Gender			
Male	38	28	34
Female	37	29	35
Education*			
High school	28	30	42
Technical	34	32	33
University	45	25	30
Posting			
At least once a day	38	25	37
At least once a week	42	25	33
At least once a month	42	25	34
Less often or never	31	35	34
Profession*			
Professional or skilled	45	28	27
Not professional or skilled	35	27	38
TOTAL (%)	**37**	**28**	**34**
TOTAL (n)	**300**	**227**	**274**

Table 5.6: 'It is acceptable for prospective employers to look at your private social media posts'

	Agree	Neither	Disagree
Age*			
Under 40	23	30	47
40–59	16	27	57
60+	20	22	58
Gender			
Male	20	27	53
Female	19	26	55
Education			
High school	16	30	54
Technical	19	30	51
University	22	23	55
posting*			
At least once a day	25	27	48
At least once a week	26	24	49
At least once a month	14	26	60
Less often or never	14	29	57
Profession			
Professional or skilled	21	28	51
Not professional or skilled	20	27	53
TOTAL (%)	**20**	**27**	**54**
TOTAL (n)	**157**	**213**	**431**

5.2 Workplace social media policies

As we will explore further below, workplace policy and government regulation of employers' access to employees' use of social media at work has not kept pace with the reality of social media usage. In the survey, we asked respondents whether their workplaces had a policy about social media use at work and individual's presentation of themselves online. While most of their employers had polices on private use, a minority had policies on the actual content of social media posting: while 72% said their workplace had 'policies or rules about using social media while at work', only 46% said their workplace had 'policies or rules about how you present yourself on the internet, for example, what you can post on blogs and websites, or what information you can share about yourself online'.

In the online discussion group, we asked participants a series of questions about how they felt about the use of social media at work, with a focus on employers accessing their personal social media feeds. Regarding whether employers should have a right to look at an employee's social media, most participants tended towards 'no'; this view was more strongly articulated when it came to 'private' versus 'public'. For example:

Personally I don't think an employer should have any control over an employee's social media. That being said, employees should refrain from any negativity pertaining to employment as social media whinging won't fix the problem. Employees in high-profile or government jobs should do the same and show common sense in what they post.

However, this was also qualified by several participants as an onus on the employee to use their 'common sense' and self-restraint. Few people believed social media should be cart blanche for employees to say what they wanted regarding their employers. And only a few people referred to the importance of a social media policy to define any boundaries and expectations of both parties. For example:

> *I don't think they should have control over what employees post in their private time … For sure. Someone working in the government would obviously have a strict guideline as to what can be posted where.*

> *I don't think any employer should have control over someone's social media or monitor it in any way [but] someone who works for the government should have common sense in regards to what they post, but so should all employees no matter where they work.*

> *I think it depends on the role the person is in … I feel people need to be smart about what they put on social media and not mention work.*

5.3 Social media and public sector employees – Australian Public Sector Commission Social Media Guidelines 2017

In August 2017, the Australian Public Sector Commission (APSC) circulated to Australian public servants (APS) a new iteration of its guidance to employees on social media use entitled *Making Public Comment on Social Media: A Guide for Employees*. The guide was the outcome of a consultation process undertaken with APS agencies and employees in late 2016. According to the APSC, the new guidelines were no more restrictive than previous policy settings, but rather addressed ambiguities and 'clarifie[d] the parameters around what public servants can and cannot say' (Lloyd, 2017).

In essence, the APS guidelines describe the dilemma as the need to balance the right of APS employees to participate in public and political debate with the statutory responsibilities of public servants of the Commonwealth, under the *Public Service Act 1999*'s Code of Conduct (section 13). The employee's responsibility in order not to act in breach of the Code, as summarised by the guide, is to 'act in a way that does not undermine the public's confidence in them and their ability to act impartially and to deliver government services professionally and without bias' (APSC, 2017, pp. 2–3).

The clarification the guide intends to bring centres around the question of what constitutes a breach versus what constitutes acceptable conduct regarding an employee's speech in the digital sphere, and in particular on social media. The key basis for distinction between offline and online comments, according to the guide, is 'the speech and reach of online communication' and the fact that 'material posted online is available immediately to a wide audience' (APSC, 2017, p. 2). In other words, since there always exists a potentially wide audience for speech online, it will be subject to a tougher protocol.

While this might sound a necessary and reasonable precaution, given the importance of APS employees being perceived to be impartial in their provision of service to the public, the APSC social media guidelines represent a significant shift in the balancing of employee rights versus responsibilities that warrants deeper consideration. Integral to this is the distinction between 'public' and 'private'. The guidelines state that, given that comments on social media involve an existing or potential audience, any comment made – even if intended as private by the employee – is in fact public. This is the case even if the person has the highest privacy settings possible, is using their own private equipment after work hours and is sending a private email to a friend:

> Public comment includes anything that you say in public or which ends up in public. This can include something you've said or written to one person. If your comment has an audience, or a recipient, it's a public comment. (APSC, 2017)

An employee may even be at risk of breaching the Code for inaction, if they fail to remove 'objectionable material' that another person posts to their page. In effect, the guidelines suggest that all social media commentary of APS employees is considered to be done in their capacity as an employee, and is therefore regulated by their responsibilities under the Act.

What about the digital rights of APS employees? Although there is currently no statutory or case law on 'right to privacy' in Australia that would limit the extent to which employer can intrude upon the private lives of their employees, to the extent that this policy has been tested for its compliance, it would seem the legality of the current APSC social media guidelines is questionable. In the recent case of *Daniel Starr v Department of Human Services* [2016] FWC 1460, the Fair Work Commission concluded that the comments made on social media by Starr, an APS employee, 'even if they are offensive, made in a private capacity but which relate to work, are not sufficient grounds for the termination of employment in the absence of some actual (rather than perceived or potential) reputational damage to the employer' (CPSU, 2017). The Commission's judgment specifically called into question the legality of the social media policy of the APSC and other corresponding APS agencies.

There is little doubt that social media communications blur the line between conventional notions of private and public, and between work and non-work life. More thinking needs to be done on how this translates into employment contexts. Currently, APS employees are being asked to bear the weight of the unresolved dilemma – of how to balance the employer's risk of reputational damage, and the employee's right to digital privacy – through the implied extension of their obligations into their personal time and their private social media use (Thornthwaite, 2013, p. 164).

Others saw it more concretely as employees having obligations, and focused on the rights of employers to monitor and control their employees' inappropriate social media use. For example:

> *They pay our wage and we should be loyal to them. We would not like our employer to damage us on social media, would we?*
>
> *I don't think an employee should comment negatively about their work. if you don't like your job, leave! They pay our wages! It's common sense.*

I think employers should monitor employees' behaviour on social media in order to mitigate any potential reputation risk, breach of data confidentiality and leakage of sensitive information.

We also asked participants to reflect on whether it mattered what kind of organisation employees worked for, particularly differences between public sector and private sector jobs. Most did not think there was a difference, as employees were entitled to privacy, but thought they should use their 'common sense' no matter what job, and employers should have clear policies. For example:

I don't think it should make any difference who you work for, your employer should not be allowed to dictate what you do in your private life, but … they do! I work for the Education Department and it is made clear to us that there are things we should not be doing with regards to social media.

The ability to complain on social media is a big yes for me, without the employer restricting what I can say, as long as I don't complain about any consequences. An employer should be very clear in an employment contract of any consequences that may be imposed if an employee states negative, slanderous or inaccurate comments that could harm the 'brand' of the employer.

I do believe they should have some control … for example if you work in the public sector and your comments could affect the work. If you use your social media at home in your own time, no they should not have any control over it. [But if you are friends with people who you work with] this could be a problem also … I know this from personal experience.

We also asked further about employers monitoring *private* social media activity of employees. Most said it was an invasion of privacy, and that there was little difference between the rights of public and private sector employees. Some qualified their answers by suggesting that people should be more thoughtful about what they post and not actually post about their employers.

I don't mix business with my personal time.

I don't think an employer should have access. But as humans if we have a problem either talk about it to friends/family/the boss or shut up.

No to both. They should not be able to have access as such, but I still believe we should not discuss our employer on any site.

No to accessing private account, but yes to a difference between public and private – might need to monitor SM accounts.

People need to be aware that anything posted on social media is never truly 'private'.

Overall, two-thirds of people believed employers shouldn't look at public social media accounts of employees, and this increased to 80% for private use. However, at the same time, there was a dominant view that the onus should be on the employee and individual choice regarding what to post about work – that is, a situation of atomised responsibility. Respondents don't seem to have equated the new work environment with the old work environment, where an employer listening to private conversations (e.g. phone tapping) would have been unacceptable; instead, they seem to have adjusted responsibility according to platform capabilities. Very few people spontaneously suggested the need for a regulatory framework or a social media policy that would outline the expectations of this relationship between employers and employees and accessing personal social media accounts.

5.4 Social media and the private sector

Social media policies are becoming increasingly common, not only in public sector agencies but also in private corporations. In December 2010, the Commonwealth Bank of Australia (now CommBank) issued a social media policy to staff which soon afterwards came under fire from the Financial Services Union (FSU) for being overly restrictive on employees' freedom of expression. The policy went beyond the regulation of commentary about the employer, customers, other employees and contractors; it also required staff to report co-workers who violated the policy. In that case, the FSU push-back was successful, as the policy was revised around mid-2011 so that employees would no longer be obliged to report on the actions of others.

In another significant Australian case, *Escape Hair Design* (2010) 204 IR 292; [2010] FWA 7358, the plaintiff had written on Facebook:

> Xmas 'bonus' alongside a job warning, followed by no holiday pay!! Whoooooo! The hairdressing Industry rocks, man!!! AWESOME!!!'

The Fair Work Commission found that, while 'foolish and silly in the context of them being made on a public forum', the comments did not justify dismissal. However, the Commissioner did say in making the judgment that, given the nature of posting online and the fact the audience to a comment cannot be controlled, '[it] is no longer a private matter but a public comment' and that 'it would be foolish of employees to think they may say as they wish on their Facebook page with total immunity from consequences' (Thornthwaite, 2013: 176).

The AIRC and FWC cases in recent years have also included cases regarding employer use of an employee's social media accounts as a source of evidence to warrant their dismissal. A 2012 survey in the United States found 'as many as 33 per cent of organizations with a social media policy had disciplined employees for inappropriate use of social media' (Lam, 2016). However, privacy arguments have not always held up in court, with a 2010 case in New York concluding that 'as neither Facebook nor MySpace guarantee complete privacy, plaintiff has no legitimate expectation of privacy … notwithstanding her privacy settings' (Lam, 2016).

5.5 Emerging issues and new platforms in the gig economy

In the project, we were also interested in assessing how digital platforms are changing the current practice and future of work, and what Australians perceive to be the risks and benefits of emerging models of platform-based work. Part of the changing nature of work is the growing precarity and insecurity of work and the workplace for a growing proportion of workers, especially younger people with limited education qualifications. We asked respondents whether they were concerned about losing their jobs due to a series of threats and changes in the nature of work. A majority were not too concerned or concerned at all about these changes and, as the list below shows, were least concerned about robots, computer algorithms and obsolete technical skills making them redundant:

- 41% were very or somewhat concerned about 'Losing your job because your employer finds someone who is willing to do your job for less money'
- 34% were very or somewhat concerned about 'Losing your job because your employer uses machines or computer programs to replace human workers'
- 30% were very or somewhat concerned about 'Losing your job because you aren't able to keep up with the technical skills required to do it'
- 28% were very or somewhat concerned about 'Losing your job or missing a job opportunity because of material posted by, or about, you on social media'.

We then asked respondents about whether they had used new gig economy platforms and what they thought about the work opportunities they presented. In our survey, we used the definition of 'gig work' as: 'These workers typically do not follow a set schedule, and get paid as they pick up assignments instead of receiving an hourly wage or salary.'

We initially asked respondents about which gig economy platforms they had used. It was discovered that

- 25% had used Uber, a ride-sharing platform similar to taxis (this rose to 43% of those under 40 and 37% of those with a degree); only 9% of respondents had not heard of Uber
- 19% had used Foodora or Deliveroo, new food delivery apps that pay workers per delivery (this rose to 30% of those under 40 and 26% of those with a degree; 31% had never heard of these new platforms
- 7% had used Airtasker, a platform to bid for one-off piece work tasks; 36% had never heard of the platform.

Respondents were asked whether they agreed or disagreed with a list of potential benefits or downsides of app-driven gig work. Nearly three-quarters of respondents shown in Table 4.7 believed that the gig economy provided workers with flexibility; however, those who were probably most likely to be in these jobs – young people aged under 40, and those with a high school level education – were less likely to agree that they were great for people who wanted flexibility. Table 5.8 shows that only 50% of respondents agreed that gig work jobs are a good entry-level job for people who are entering the workforce. Again those with a high school level education were least likely to agree with this proposition.

Table 5.7: Gig work jobs are great for people who want a flexible schedule

	Agree	Neither	Disagree
Age*			
Under 40	66	26	8
40–59	76	22	2
60+	72	26	1
Gender			
Male	68	27	5
Female	75	22	4
Location			
Capital city	73	22	5
Not capital city	69	28	3
Education*			
High school	64	34	3
Technical	69	25	6
University	78	17	4
TOTAL (%)	**72**	**24**	**4**
TOTAL (n)	**573**	**195**	**33**

Table 5.8: Gig work jobs are a good entry level job for people entering the workforce

	Agree	Neither	Disagree
Age			
Under 40	52	36	13
40–59	51	39	10
60+	45	47	7
Gender			
Male	49	41	10
Female	50	39	10
Location			
Capital city	52	37	11
Not capital city	46	44	10
Education*			
High school	40	52	8
Technical	55	36	9
University	53	34	13
TOTAL (%)	**50**	**40**	**10**
TOTAL (n)	**399**	**319**	**83**

Yet when we asked respondents whether gig work provided career opportunities the numbers agreeing dropped to 29% in Table 5.9, but university-educated, and those living in capital cities were significantly more optimistic about careers from gig work.

We also asked about a potential downside to gig work (Table 5.10) – whether it leaves workers financially insecure. Only 13% of respondents disagreed, with 41% agreeing and the remainder neither agreeing nor disagreeing. University educated people and those under 40 were significantly more likely to agree that gig work was financially insecure. As it is a relatively new phenomenon, there is a great deal of uncertainty among our respondents about what gig work might provide for workers. For more secure and older workers, it may also not be a scenario they have thought about much, as it is neither work they will do nor a service they have used.

Table 5.9: Gig work jobs are the kind of jobs you can build a career out of

	Agree	Neither	Disagree
Age			
Under 40	31	40	29
40–59	30	47	24
60+	27	51	22
Gender			
Male	30	44	27
Female	29	46	24
Location*			
Capital city	32	42	26
Not capital city	25	51	25
Education*			
High school	26	56	19
Technical	30	48	22
University	32	37	32
TOTAL (%)	**29**	**45**	**25**
TOTAL (n)	**236**	**362**	**203**

Table 5.10: Gig work jobs leave workers financially insecure

	Agree	Neither	Disagree
Age*			
Under 40	47	40	13
40–59	43	47	11
60+	31	54	15
Gender			
Male	41	46	13
Female	42	46	13
Location			
Capital city	43	44	13
Not capital city	39	48	12
Education*			
High school	36	54	10
Technical	32	55	13
University	51	35	14
TOTAL (%)	**41**	**46**	**13**
TOTAL (n)	**332**	**367**	**102**

As we were also interested in regulation of and for digital rights, we asked respondents about what kind of regulation might become necessary for workers in the online gig economy. Table 5.11 shows that 61% thought new regulations were necessary, although these were evenly split between a fully regulated gig economy and those who thought regulations should focus mainly on employment relations. There were few demographic differences between these two forms of regulation, except that people over 60 were slightly more in favour of employment-focused regulations. As we were asking about government regulations, we also looked at whether political partisanship made a difference to what kind of regulation was preferred. There were no differences between major party preferences, but Greens identifiers were the group most likely (45%) to favour new employment-related regulations for the gig economy.

Table 5.11: **Which ONE of the following statements about government regulation of any of these online gig work platforms do you agree with most?**

	Fully regulated	New employment-related regulations	No new regulation	Unsure
Age*				
Under 40	34	31	13	21
40–59	29	28	7	36
60+	28	34	11	26
Gender				
Male	30	31	12	27
Female	31	31	9	29
Location				
Capital city	32	31	10	27
Not capital city	28	31	11	30
Education*				
High school	28	28	7	38
Technical	30	29	12	30
University	33	34	12	21
Party*				
Labor	33	30	7	30
LNP	33	35	13	19
Greens	23	45	10	22
Other	33	28	15	24
None/DK	26	24	11	39
TOTAL (%)	**30**	**31**	**10**	**28**
TOTAL (n)	244	247	84	226

5.6 Regulating gig workers' rights

Whether labelled the 'sharing', 'on-demand', or 'gig' economy, communication technology transformations are restructuring the labour market and changing the way people work. With digitally mediated platforms facilitating interaction between individual consumers and corporations, Uber, Airtasker, Foodora and Amazon Mechanical Turk are 'brokering' a new workplace infrastructure. While the nature and terminology of this form of digitised work vary widely, the 'gig' economy is typified by several common features, including irregular hours driven by consumer demand, compensation on a piecework basis rather than a set salary, worker-supplied equipment and/or workplace, and the mediation through a digital platform or app (Stewart & Stanford, 2017). While precarious work featuring irregular hours and piecework compensation is not a new phenomenon (Lewchuk, 2017), the scale and ubiquity of the online gig economy creates additional issues for regulators and policy-makers (Stewart & Stanford, 2017). As much as these developments are heralded by some as cutting transaction costs and reducing barriers to entry into work, they are coming under increasing scrutiny in relation to the casualisation and informalisation of work (De Stefano, 2016), as well as worker rights and labour market regulation.

Uber was founded in 2009, and grew exponentially from an entrepreneurial start-up to a multibillion dollar multinational corporation (Martin, 2016). It is now the world's largest ridesharing company, which has seen its operations spread to almost 70 countries. Uber's business model is based a network of 'partner-drivers', who are deemed 'independent contractors' rather than Uber employees (Stewart & Stanford, 2017). In the United States, for example, Uber claims that its platform and others like it are 'boosting the incomes of millions of American families. They're helping people who are struggling to pay the bills earn a little extra spending money or transitioning between jobs' (Aloisi, 2016, note 81). However, Uber drivers in America not only pay their own insurance, maintenance and petrol costs; their right to drive can be terminated at any time by the company and rates changed without notice. Furthermore, they are not covered by any existing US employment law such as minimum wage, overtime or anti-discrimination legislation (Aloisi, 2016, p. 673). Uber therefore exhibits an unusual degree of control over its 'partner-drivers' in a manner that is not common elsewhere in the gig economy (Stewart & Stanford, 2017, p 424).

In a 2015 class action lawsuit brought to the Northern District of California Court, four Uber drivers sued the platform on the basis that they were employees under California law, and that, as such, Uber had violated the California Labor Code. The dispute centred on whether the drivers were employees of Uber or 'independent contractors'. This question, in turn, rested in large part on how Uber should be characterised under the law. While Uber referred to itself as a 'technology company', and not as a 'transportation company', the plaintiffs disagreed, pointing to Uber's previous references to itself as an 'on-demand Car service' or 'everyone's private driver'. Set for trial in June 2016, the Californian case was settled; however, the issue of classification of drivers and of Uber itself remains unresolved (Aloisi, 2016, p. 677). The case demonstrates an issue arising in jurisdictions elsewhere, including Australia, in which labour laws developed over the last century because of industrial action by trade unions and others – such as minimum wage rates and minimum work hours – do not apply to workers not deemed under a 'contract of service'. In other words, while decent wages and working conditions are a fundamental right of workers under the International Labour Organization's (ILO) constitution (Riley, 2017, p. 5), the legal manipulation of these commercial arrangements has seen a growing number of workers fall into a regulatory 'black hole', and into conditions that reflect a form of subjugated labour. Many drivers have been found to rely upon Uber as their main source of income, meaning that regulation of the gig economy workforce and of the terms and conditions of their work is vital (Riley, 2017, p. 5).

Most attempts to regulate Uber – which may or may not include protections of its drivers – are happening at the state level in Australia. For example, in Victoria there has been an attempt to regulate non-employed labour engagement contracts in the road transport industry via the existing *Owner Drivers and Forestry Contractors Act 2005* (Vic), with provisions that might be adapted to the needs of rideshare drivers. This includes standardising fares and compensation for costs borne by drivers, such as motor vehicle expenses, or a telecommunications provider's charges for accessing the large amounts of data required to operate the app. These changes will not establish Uber drivers as employees, but may mitigate some of the current risks and lack of entitlements in their work arrangements (Riley, 2017).

Chapter 6

Speech

Core findings

- Australians are not strongly wedded to the North American ideal of absolute speech freedom online. Just over one-third (37%) of those surveyed agreed that they should 'be free to say and do what I want online', but 30% disagreed and one-third expressed reservations about the idea. People were also less supportive of others having that absolute freedom than themselves.
- Around half of the respondents agreed that everyone should have the right to online anonymity or pseudo-anonymity, a figure that increased to 57% for those under 40 years. Around one-third of younger Australians said it was more likely that they would make honest and open comment on the news, talk about sensitive topics like sexuality or question others' opinions if they had the opportunity to comment anonymously.
- Men were more likely to assert their right to free expression than women, reflecting the male dominance of everyday speech online as much as offline.Gender is a key variable in understanding attitudes to social media regulation. Men were less likely than women to agree with the need to remove instances of sexual harassment, abuse targeted at an individual, or hate speech that encourages violence against others within 24 hours. Women were less supportive than men of the right to anonymity.
- While most respondents had not experienced negative impacts from risky or harmful online speech, 39% had been affected by mean or abusive remarks and 27% had experienced personal content posted without consent. Our case study on image-based abuse emphasises the need for law reform and educational strategies to address new privacy and speech rights breaches.
- More than occurred for either work or privacy issues, respondents agreed that there should be more regulation of online discussion environments. They flagged the need for increased involvement by social media platforms in content moderation and 'easy' complaints reporting.
- There was a perception gap between people's belief that harmful social media content was easy to get taken down and the procedural reality that it was not always straightforward and may require regulatory intervention to persuade the host company to act, as the European Commission hate speech case study (discussed below) suggests.

6.1 Online speech rights

Over the last decade, studies of the scope of online abuse in Australia (Henry, Powell & Flynn, 2017; Katz et al, 2014; Powell & Henry, 2015), together with high-profile examples of hate speech, cyberbullying and 'revenge porn' or image-based abuse, have underpinned calls for new approaches to controlling harmful speech online and to educating people about what is respectful, inclusive public talk.[1] How Australians understand their speech rights, and what they think it is appropriate to say online, constitute important territory for digital rights research to explore, given that millions of us are now social media publishers and legally responsible for what we say in these environments. As Chapter 5 outlined, Australian employees are increasingly subject to workplace codes governing what is acceptable online speech, even when they are communicating via ostensibly private social media accounts. Yet questions remain about what we should and shouldn't say online, and who – if anyone – should regulate our talk, and these issues often spark polarised debates.

On one end of the speech rights spectrum are those who believe early, largely North American, claims for the internet as a space for absolute free speech (Barlow, 1996; De Sola Pool, 1983), beyond even the limited confines of the US First Amendment. On the other end of the spectrum are advocates and institutions seeking regulatory means to limit the tides of hate speech and gender discrimination online, and demanding new forms of platform accountability for content filtering. Recently, however, the balance has tipped towards those who are calling for regulatory reform. On 31 May 2016, for example, the European Commission entered into the Code of Conduct for Countering Illegal Hate Speech Online with Facebook, Twitter, YouTube and Microsoft (the provider of corporate social services such as LinkedIn and Yammer). A key feature of this Code was that the major social media platforms committed to take down formally reported instances of hate speech within 24 hours (European Commission, 2016b). Our research, then, comes at a crisis point in the free internet speech narrative – a moment where even US IT companies like GoDaddy and Google, which ordinarily would be strong free speech proponents, have refused to host neo-Nazi sites in the wake of white supremacist demonstrations (Mettler & Selk, 2017). In this moment, we set out to explore what speech rights Australians value, how they have been affected by risky or harmful behaviours and who they believe should take responsibility for monitoring and regulating online speech.

Australian attitudes are interesting to canvass precisely because there is no constitutional right to free speech in this country. Instead, Australia has developed a complex series of laws and regulatory strategies to ensure 'positive' speech rights – that is, to protect against the risks and harms of uncontrolled speech. Australian law prohibits the posting of illegal or offensive content online that would be 'refused classification' under the *Classification (Publications, Films and Computer Games) Act 1995* (as set out in the Online Content Scheme, schedules 5 and 7 of the *Broadcasting Services Act 1992*). Australia also works to prevent reputational damage via defamation law, and racial vilification and cultural discrimination at both the state and federal levels.

Most recently, the national Office of the eSafety Commissioner was established under the *Enhancing Online Safety (Intimate Images and Other Measures) Act 2015* (Cth) (formerly the *Enhancing Online Safety for Children Act 2015* (Cth)). Initially, the eSafety Commissioner had the power to ask individuals, or the social media platforms on which they post, to remove 'serious cyberbullying' material that targeted an Australian child and was likely to seriously threaten, humiliate, harass or intimidate them. In May 2017, a legal change gave the Commissioner responsibility for all Australians, with a focus on people at risk of family or domestic violence, older Australians and those at risk of having intimate images of them shared without their consent. In total, this regulatory breadth means that Australian internet users are likely to have some sense of the ways in which speech rights are limited and why regulation might be necessary to support inclusive, civil speech online.

As a starting point to exploring attitudes to communicative rights, we began by probing how people saw their rights to free speech in relation to others, and the importance that they might place on having certain types of digital liberties, such as the right to anonymity online, or the right to speak their mind on particular issues such as government, religion and political extremism.

6.2 Attitudes to speech rights

We found that Australians are not wedded to the strong, North American idea of free speech online. When asked how strongly they agreed with the statement that 'I should be free to say and do what I want online' (Table 6.1) opinion was divided. Over one-third (37%) of respondents thought they should have that absolute freedom, but 30% disagreed and a third expressed reservations about the idea, by choosing 'neither'.

Table 6.1: I should be free to say and do what I want online

	Agree	Neither	Disagree
Age*			
Under 40	50	38	12
40–59	30	34	36
60+	27	26	47
Gender*			
Male	43	31	27
Female	31	36	33
Party*			
Labor	41	27	32
LNP	26	33	41
Greens	42	34	24
Other	42	29	29
None/DK	37	41	22
TOTAL (%)	**37**	**33**	**30**
TOTAL (n)	**295**	**267**	**240**

There were some clear demographic differences of opinion. Those under 40 were more solidly in favour of free speech conditions for themselves (50% agreed, 12% disagreed), while those over 60 were less enthusiastic (27% in favour, 47% against). Men were more in favour of untrammelled speech for themselves (45%) than women (33%). Those identifying with Labor, the Greens and minority parties were more in agreement with free speech rights than Liberal/National identifying respondents.

Table 6.2 shows that, predictably, people were more likely to favour regulation of others' speech than their own. Some 33% agreed others should have that absolute freedom, but 35% disagreed. Those under 40 were still more strongly in favour of free speech conditions for all (49% in favour, 16% opposed), while those over 60 were more clearly in favour of some form of regulation (26% in favour of free speech for all, 57% against). Again, men were more in favour of free speech conditions for all (42%) than women (27%). This gender discrepancy is perhaps to be expected, given that research here and overseas has shown that women, more than men, tend to be the target of cyberbullying and sexualised harassment or abuse (Bartlett et al., 2014; Katz et al., 2015). Again, Liberal/National Party identifying respondents were less in agreement about free speech rights for others than were other partisans.

Table 6.2: Everyone should be free to say and do what they want online

	Agree	Neither	Disagree
Age*			
Under 40	46	39	15
40–59	24	33	42
60+	26	19	56
Gender*			
Male	40	29	31
Female	26	34	40
Party*			
Labor	33	34	33
LNP	25	28	46
Greens	39	26	35
Other	40	25	35
None/DK	34	38	28
TOTAL (%)	**33**	**32**	**35**
TOTAL (n)	**264**	**255**	**283**

The members of our online discussion group were largely supportive of the principle of free speech online, saying variously that there should be 'total freedom' of expression, 'open slather' or 'no restrictions' placed on discussions. However, half the respondents noted key instances where they thought there should be regulation – for example of hate speech, discrimination or bullying:

> *I think you should be able to have freedom of speech online but so many people cross the line and put way too much out there … Discrimination, racist comments should be censored.*

Importantly, half our survey sample agreed that everyone should have the right to 'anonymity' online (Table 6.3), a term that we also took to include the capacity to post using a nickname or pseudonym – as distinct from the real-name identity systems of Facebook, Wechat and Google Plus.

Table 6.3: Everyone should have the right to anonymity online

	Agree	Neither	Disagree
Age*			
Under 40	57	30	12
40–59	41	36	24
60+	49	30	21
Gender			
Male	53	30	17
Female	46	33	20
Posting*			
At least once a day	60	27	12
At least once a week	53	31	17
At least once a month	53	24	23
Less often or never	40	42	18
TOTAL (%)	**50**	**32**	**19**
TOTAL (n)	**397**	**256**	**149**

People under 40 were more likely to support anonymity (57%) than those over 60 (26%), possibly because they were more concerned than older people about being judged by their peers. Further, given that Chapter 5 notes concerns about employers seeking access to employees' real name social media accounts, then anonymous or pseudonymous social media may represent a haven from this form of surveillance.

Men were more likely to agree with the right to anonymous posting (40%) than women (26%), raising the question of whether Australian women are more concerned than men about the potential to be targeted by anonymous threats when they speak publicly. We also found that those who posted most often were more supportive of the right to anonymity than those who posted less frequently, which correlates with studies linking the provision of anonymity and pseudo-anonymity with the likelihood of participation. However, when we asked whether Australians wanted the right to anonymity in order to talk about particularly controversial topics, we found that most people (between 62% and 68% of respondents) reported it would make little difference – except for people under 40 years. Some 38% of younger Australians said they were more likely to post honest and open views on the news if they had anonymity, while 30% were more likely to talk about sensitive topics like sexuality and 35% to question others' opinions. For around a third of young Australians, the possibility of posting under an assumed name may enable more authentic participation in public debates.

When we explored what types of critical statements people felt they should be able to make openly and freely online (Tables 6.4 to 6.7), we found that most of our respondents agreed that people should be able to criticise government policies (56%). Older Australians and men were more inclined than younger people and women to agree that this was important, possibly

reflecting their greater participation in, and control of, traditional political organisation. Interestingly, the least support for this critique came from Liberal/National voters – traditionally supporters of free speech principles – and the greatest support came from supporters of the Greens and minor parties.[2]

Table 6.4: Criticisms of government policies

	Agree	Neither	Disagree
Age*			
Under 40	50	38	13
40–59	56	31	13
60+	65	23	12
Gender*			
Male	63	28	9
Female	49	35	16
Party*			
Labor	59	26	15
LNP	55	30	16
Greens	72	27	1
Other	71	24	5
None/DK	43	42	15
TOTAL (%)	**56**	**31**	**13**
TOTAL (n)	**448**	**252**	**102**

There was less enthusiasm across the board for the right to criticise religious organisations (31%) or minority groups (26%), and feelings were polarised about these propositions, with over one-third of respondents in each instance disagreeing that people should be able to make these types of statements online. There was little difference in opinion about these positions across the survey group in terms of age, location, educational background, or frequency of posting, showing that these are very commonly held attitudes. Men were slightly more likely than women to agree with people's right to religious and minority group critique. Minority party partisans were more likely to agree with criticism of religion and minority groups.

Table 6.5: Criticisms of religious organisations or religious beliefs

	Agree	Neither	Disagree
Age*			
Under 40	30	42	28
40–59	29	35	35
60+	33	27	39
Gender*			
Male	38	34	28
Female	24	37	39
Education			
High school	29	41	30
Technical	32	31	37
University	32	35	34
Posting			
At least once a day	32	35	34
At least once a week	30	42	28
At least once a month	37	30	33
Less often or never	25	38	37
Party*			
Labor	31	31	36
LNP	32	30	37
Greens	36	42	22
Other	43	29	28
None/DK	22	44	34
TOTAL (%)	**31**	**36**	**34**
TOTAL (n)	**247**	**286**	**269**

Table 6.6: Criticisms of minority groups

	Agree	Neither	Disagree
Age			
Under 40	24	40	36
40–59	25	39	37
60+	30	32	38
Gender*			
Male	32	38	30
Female	20	37	43
Location*			
Capital city	26	34	39
Not capital city	25	43	32
Education*			
High school	23	43	34
Technical	29	40	31
University	26	32	42
Posting			
At least once a day	26	35	39
At least once a week	30	39	31
At least once a month	27	37	36
Less often or never	17	42	41
Party*			
Labor	27	33	40
LNP	29	39	32
Greens	23	31	46
Other	44	28	28
None/DK	16	46	38
TOTAL (%)	**26**	**37**	**37**
TOTAL (n)	**208**	**300**	**294**

There was little taste for the right to make explicit sexual statements or to call for violent protests. Only 11% of the cohort agreed that people should be able to make these kinds of statements online, with men being slightly more in favour of explicit sexual talk than women (19% compared with 9%) and those under 40 being more in favour of calling for violent protest (20%) than those

over 60 (3%). Most people surveyed disagreed with the notion that people should be able to use the internet to encourage non-violent action that breaks laws they believe are wrong (Table 6.7). However, nearly a quarter of the population (23%) thought people should be able to do this. Frequent posters (32%) and Greens supporters (43%) were most in agreement with this principle, while older Australians (42%), Liberal/National and minority party supporters disagreed (46%).

While the political polarisation is not unexpected, this finding indicates that some internet user groups value the possibility to call for non-violent political action, even where the majority disagree with that action. Also, as daily posters – those most engaged in social media talk – were more likely to agree with this notion than those posting once a month or less, we could also raise the question of whether there is a link between the degree of online participation and interest in testing legal and political boundaries.

Table 6.7: Encouraging non-violent actions that break laws the person believes are wrong

	Agree	Neither	Disagree
Age*			
Under 40	28	45	27
40–59	21	37	42
60+	20	38	42
Gender			
Male	25	37	38
Female	22	44	34
Education			
High school	19	43	38
Technical	24	41	36
University	27	38	35
Posting			
At least once a day	32	36	32
At least once a week	23	43	34
At least once a month	25	37	38
Less often or never	19	44	37
Party*			
Labor	27	41	32
LNP	21	34	46
Greens	43	36	20
Other	23	31	46
None/DK	16	50	33
TOTAL (%)	**23**	**40**	**36**
TOTAL (n)	**188**	**323**	**291**

In every instance of our speech rights questions, men were more likely to assert their right to free expression than women, reflecting the male dominance of everyday speech environments online as much as offline. Thus, despite initial hopes that the internet would develop as an arena for more equitable communicative rights, our study suggests men are still more likely than women to feel confident to express their rights to free speech online.

On a more positive note, the survey suggests that people understand the distinction between the need to enable speech that criticises government and to regulate speech that criticises minority groups or incites violent protest. This suggests a relatively sophisticated understanding of free speech conditions, and the means to build a fair, inclusive political culture online. We can also look, for example, to the small support for speech that condones non-violent law-breaking where there is a moral justification, to see how the internet provides a forum for political dissidence that would not be supported by mainstream media. Indeed, our discussion group argued that media workers should be subject to tighter speech regulation and more accountability online than ordinary citizens, with an emphasis on ensuring accuracy and balance or impartiality:

> *Yes, there should be total freedom online [but] I would support restrictions around media sites (not social media, but the real media) and government, etc. Media needs to be held to higher account, and factual correctness than just blogs/Twitter, etc., when voicing opinions.*

> *I believe stricter rules need to be in place for media. Which does need to be more impartial/moderate in their views (on news sites, etc.).*

With these outcomes in mind, it is important to ask whether it is due to our weak constitutional rights framework that people have been forced to develop a more nuanced imaginary of what is acceptable 'free speech' than we find realised in the more polarised freedom or censorship arguments that have played out in the United States.

6.3 The impacts of risky and harmful behaviours

While Australians have a robust legal framework for dealing with some forms of harmful and offensive speech, such as defamation or discrimination, our legal systems do not necessarily help us to negotiate what to do about everyday incivility: 'mean speech', occasional unwanted contacts, discrimination masquerading as humour, ad hominem attacks and other forms of rude, aggressive behaviour. Australian law is yet to adequately address other new and more serious forms of online harassment such as doxing (publishing online private material about someone for malicious purposes) or swatting (impersonating someone in order to perpetrate a hoax and humiliate the victim). Further, the laws regarding another new form of visual threat, image-based abuse, are also inconsistent between Australian jurisdictions.

In this research, we wanted to explore the incidence of some of these behaviours alongside more serious forms of assault to get an idea of how they might be affecting

people's interactions and their capacity to express themselves safely and confidently. We also wanted to find out how risky and harmful speech affected people's publishing activities and those of any children in their families, and how they responded to that behaviour.

When we looked at the risks of people being exposed to abusive or negatively intrusive speech behaviours on social media platforms and elsewhere online, we found that, overall, the majority of Australians have escaped these experiences – or, rather, that they have not affected their online interactions (Table 6.8). We wanted to distinguish behaviour experienced from that which affects further online interactions, as we are interested in charting the impact of negative and risky behaviours on speech rights. We also found that, with one exception, there was little difference between the degree of abuse, insult or offence that women and men reported affecting their online interactions – even in regard to unwanted sexual contact.

While these are positive findings, it is important to note that the online activities of 39% of the Australians surveyed have been affected by mean or abusive remarks online. A fifth of respondents have been affected by racist comments or unwanted sexual contact (including sexting and solicitation), with men reporting more experience of racism and both genders reporting a similar degree of unwanted sexual contact. Just under one in five respondents had been affected by trolling, harassment and bullying. Significantly, this was far more likely to affect those respondents in the younger age brackets (from 33% of those under 30 years to 7% of those over 60).

An interesting finding was that one in four respondents (27%) had experienced personal information posted without their consent – the only category of harmful speech where women experienced this more than men, although this may have been because the posting of children's photographs without consent was used as the example. While Australian schools have introduced strict controls around the taking and publication of images of children, the social conventions around everyday social media circulation of adults' and children's images are not yet clearly established.

Table 6.8: Behaviours that have affected online interactions

Behaviour	Yes
Mean or abusive remarks	39%
Personal information posted without permission by others (e.g. children's photos)	27%
Unwanted sexual contact (sexts, solicitation)	20%
Racism	20%
Trolling, harassment or bullying (sustained abuse)	18%
Impersonation or swatting (hoax calls made in your name)	13%
Personal information exposed deliberately or maliciously (doxing)	12%
Violent sexual contact (revenge porn, sexualised threats)	6%

To a large extent, the overall survey figures in Table 6.8 parallel the findings of the international Microsoft Digital Civility Index 2017, including research conducted among adults and teenagers in 14 countries. The exception to those findings is that Australians say they are more affected by impersonation or swatting than those surveyed in other countries (13% in our survey as compared with 3% in the Microsoft survey).

The impacts of online impersonation can range from minor inconvenience, such as hoax business orders or fake profiles, to serious legal entanglement – for example, where someone contacts the police to claim that their target is perpetrating a crime such a murder or hostage-taking. It can also involve sending offensive emails from a victim's account or creating fraudulent accounts in the victim's name, and using them to embarrass or humiliate that person. Originally seen as a form of hoaxing or prank, in the United States swatting has been labelled as a new form of cyberbullying (Jaffe, 2016). Like doxing, which in this survey affected a similar number of respondents (12%), and image-based abuse, which was relatively rare among our survey group, swatting is a relatively new phenomenon, which has a range of implications for digital rights, platform complaints and the legal process.

It is also clear that these harmful behaviours are affecting our participation in online talk and our engagement with social media platforms. We asked respondents whether they had ever reduced their comments on social media due to other people's behaviour, or advised their children to reduce their social media use due to other people's behaviour. Over one-third of parents or guardians (37%) have advised their children to reduce their social media use due to the behaviour of others, and 34% have reduced their own use. We also asked whether they had deleted a social media account due to abuse or bullying, or advised their child to do so. Nearly one-quarter of those surveyed (24%) had advised their children to delete a social media account due to bullying, and 16% had deleted one of their own accounts.

This incidence of retreat from social media interaction underscores the need for new regulatory strategies and other forms of social intervention to reduce the most serious forms of harmful speech. In the first of our our open survey questions, trolling and other forms of aggressive and harmful speech were listed as the third most important political, social or legal issue with internet and digital technologies that needed to be addressed in the next five years. Successive Australian governments have certainly supported anti-cyberbullying initiatives over two decades, and there is now a strong push to develop measures to combat image-based abuse, but this report also indicates the need for a broader set of educational measures to:

- support the reduction of everyday mean talk, and introduce strategies for learning constructive argument – especially for young people

6.4 The case for rights education and law reform to tackle image-based abuse

As online communications increasingly focus on visual representation, we are seeing a rise in the illegal distribution of sexual and/or intimate images and recordings without the subject's consent, as well as the dissemination of faked intimate images. A recent study of image-based abuse notes that our understanding of this behaviour should extend well beyond the common label of 'revenge porn' to include any use of photos and videos of a sexual nature 'to coerce, threaten, harass, objectify' and denigrate someone (Henry, Powell, & Flynn, 2017, p. 3). As the eSafety Commission noted in its submission to the Commonwealth Senate Legal and Constitutional Affairs References Committee inquiry, 'non-consensual sharing of private sexual images can be a form of family violence or sexual abuse, and can also constitute cyberbullying material, and in the case of minors, child sexual exploitation material' (Office of the Children's eSafety Commissioner, 2016).

Image-based abuse breaches users' privacy rights and can curtail their speech freedoms, particularly where the abusive behaviour publicly shames the victim or mobilises a backlash against them. Some 76% of those who have experienced this abuse and were later surveyed by the eSafety Commissioner did not take action to remove the images – 29% because they felt it wouldn't change the situation, 22% because they didn't know what to do and 29% because they felt too embarrassed or ashamed to act (Office of the eSafety Commissioner 2017).

In late 2017, the eSafety Commissioner launched an educational website to support Australians in identifying, reporting, removing and prosecuting image based abuse. This type of resource is critical for educating people about their rights to take action against perpetrators, as well as to suggest ways to collect and present evidence to a social media service or authorities. Importantly, it recognises the diversity of people affected by this type of attack, and offers tailored support advice for the LGBTQI communities and Indigenous Australians, who are disproportionately highly represented in statistics on this abuse.

For those seeking legal redress, at present there is no specific national law designating this type of abuse as a criminal offence. Section 474.17 of the Commonwealth Criminal Code 1995 does however prohibit misuse of a carriage service to menace, harass or cause offence, and carries a maximum penalty of three years' imprisonment. According to the Minister for Women, Senator Michaelia Cash, 'there have been a number of successful prosecutions for revenge porn' using this provision (Goldsworthy, 2017). The Australian Government intends to introduce a civil penalty regime by the end of 2017, to be administered by the eSafety Commissioner. While not involving criminal prosecution, civil penalties may include fines, injunctions and enforceable undertakings that hopefully will speed up the removal of offending images (Department of Communications and the Arts, 2017).

In the meantime, while most Australian states and territories have criminal provisions to prohibit certain forms of image based abuse, some do not. As of November 2017, New South Wales, the Australian Capital Territory, Victoria, South Australia and Western Australia had all enacted new, specific criminal provisions relating to image-based abuse, while Queensland, the Northern Territory and Tasmania had not. In those jurisdictions without specific provisions, victims may be able to prosecute individuals for more general offences, such as stalking and harassment.This apparent legal inconsistency is exacerbated by the often complex cross-jurisdictional, transnational nature of image-based abuse (and online publishing more broadly). It is much more difficult to prosecute or remove content posted by actors overseas, hosted on servers outside Australia, in countries with no legal framework for recognising these acts of violence. The cross-jurisdictional dilemma for law-makers was raised during our discussion group, with one participant asking how regulation of speech on social media could proceed when so many disparate actors, legal systems and territories are involved:

> *'Who would create the rules and who would police them? The trouble with the Internet is that it is global, so rules and country legal boundaries can get blurred. If I post something on Facebook, is it governed by the rules of Australia (where I posted it) Singapore (where the server is), the USA (Facebook HQ) or elsewhere?'*

- explore what constitutes racist and sexually discriminatory or intimidatory talk, and how it can be countered.
- raise the serious impacts of impersonation and hoaxing.
- highlight issues of consent to post images or personal information about others.

More broadly, governments and civil society organisations need to consider the implications of having private companies determine what is acceptable, fair and inclusive public talk, and to explore ways in which they can collaborate on research, education and regulatory measures.

6.5 Online content regulation

Until recently, social media companies had carefully resisted calls to directly moderate the content they hosted, preferring to 'empower' people to control their reception of inappropriate communications by hiding offensive posts and banning or blocking certain users, as well as giving individuals reporting tools to flag problematic content. However, the growth in online misogyny and violent, sexualised harassment, the use of live streaming tools to represent murder or suicide online, and the rise of neo-Nazism and Islamic state terrorism have all led Western platforms like Facebook, YouTube, Instagram and Twitter to entertain new possibilities for content regulation. These include Facebook CEO Mark Zuckerberg's 2017 promise to hire 3000 more moderation staff, and Alphabet and Facebook's research into machine learning strategies for filtering written and visual content.

In our final set of survey questions, we explored Australians' attitudes towards the need for content regulation on social media platforms, together with their experiences of, and beliefs about, content regulation. We first asked people to prioritise the forms of speech that they most wanted regulated, so our respondents were asked to nominate how important it was that certain types of harmful and risky content were removed from social media within 24 hours of posting.

The types of content that most troubled people were, in order, sexual harassment (88% agreed or agreed strongly that this should be removed quickly); abuse targeted at an individual (87% agreed in total); and hate speech that encourages violence (86% in total agreed). There was a somewhat lesser, but significant, concern about the removal of sexually explicit talk (74% in total agreed) and extremist political talk (73% in total agreed). In both those instances, people under 40 thought it less important to take action on these types of speech than those over 60. Otherwise, there were very few demographic differences in terms of location, educational background, frequency of posting or political affiliation in people's judgement of speech risks.

In summary, people were overwhelmingly agreed on the need for quick action to address harmful or risky content. The exception to this trend was people's attitudes to anti-government talk. Overall, only 37% of the survey respondents thought this should be addressed by fast removal, although this percentage may have been somewhat boosted by its placement alongside other more harmful speech acts. Even so, it corresponds with the earlier finding about support for speech that criticises government and signals a healthy interest in robust political talk.

Significantly, though, without exception men were less concerned about the need to remove harmful content more quickly than women. The difference was marked in relation to removal of:

- abuse target at an individual (81% of men agreed this was important compared with 94% of women)
- sexual harassment (83% of men agreed versus 93% of women)
- hate speech that encourages violence (79% of men agreed versus 92% of women)
- sexually explicit talk women (64% of men agreed versus 85% of women).

Gender, then, is a key variable in understanding attitudes to social media regulation. Given that men play a key role in the design, development and operation of social media platforms, and are dominant in executive positions, it seems important to examine how gendered attitudes to content moderation influence corporate strategies, policies and practices.

Despite the keen concern survey respondents showed toward regulation of dangerous or risky speech, and the relatively common experience of abuse and mean speech, very few of our respondents said they had used a reporting function on a website or app to complain about inappropriate or offensive content. This lack of experience in reporting offensive content gives some context to our online group discussion, which explored how people would go about getting offensive and hateful content removed from social media feeds and web sites.

The majority of focus group respondents said they thought it was 'easy' to get offensive and hateful posts removed from social media and websites, noting that 'there is plenty of help from different sites to have things taken down'. However, some comments suggest respondents were talking about filtering content – that is, hiding or blocking posts from their personal feeds – rather than having them taken down. Several respondents noted that the ease of having inappropriate content removed was contextual and depended on the administrators' judgement and the host service process:

> *I know for a fact it isn't very easy, it may be easy to complain but most of the time the administrators don't find it offensive and leave it.*
>
> *It's easy to remove and block things on Facebook, sometimes it's as easy as clicking an option, Google is a bit harder if you want to remove a photo it is a process can take up to four weeks.*
>
> *Depending on the platform it can range from extremely difficult to just difficult, not easy at all. A more simple and easy to follow process should be created with the big social media companies coming up with a set of guidelines (wishful thinking). If the offensive post was from a fake account (i.e. not from a confirmed person) then the post should be easy to remove, if it's from a confirmed real account then the person that posted it should be given the opportunity to remove it and have it explained why it needs to be removed.*

When asked who they would approach to remove a hateful or offensive comment if the author refused to delete it, 11 of 14 respondents nominated site administrators as having the primary role in addressing complaints. However, there was also a majority willingness to have police involved if the matter was serious and the request for removal of content could not be resolved. As one respondent said, 'the more complaints they get the sooner they will have to put procedures in place to deal with it'. Another respondent noted that the response would 'depend on what they said and what my rights were'.

Our group discussion participants unanimously agreed that it was the responsibility of the platforms, rather than government or individuals, to monitor and proactively remove hateful or offensive content:

> *Facebook and social media companies have a responsibility to remove offensive comments and behaviour on their sites. It is easier if they remove it and monitor it and deal with it. It's important they deal with it so they don't encourage bad behaviour on their social media sites.*

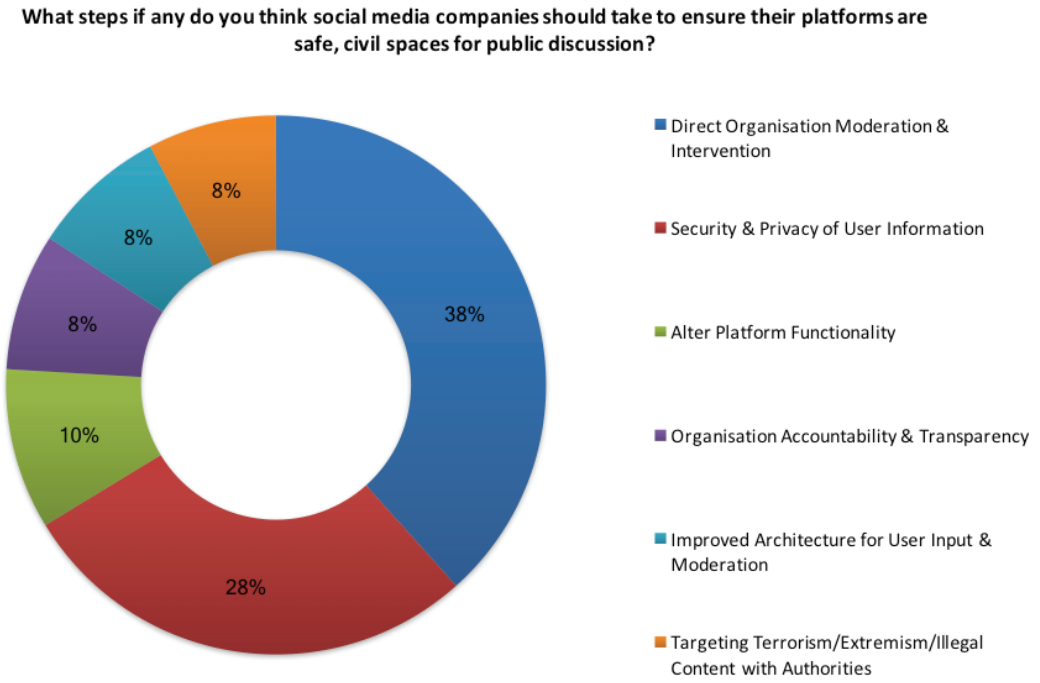
> *It's up to the people who run the social media. They review problem posts and make a decision.*

> *I think administrators are and should be responsible for monitoring such posts … I don't really think government regulators should be involved other than in extreme circumstances. And yes, I believe social media platform users should have a say – we are, after all, the user.*

Four of our group members argued that individuals must be responsible for what they posted, but none indicated that that this mitigated the need for social media platforms to monitor and moderate content. Six of 14 discussants also raised the possibility of a government department/ombudsman/watchdog/independent mediating body being set up to deal with content removal requests, although there was some ambivalence from other respondents regarding any government intervention in content regulation. One discussant also raised the possibility of 'robots' monitoring speech standards, which suggests public recognition of the new artificial intelligence software being trialled by Google and Facebook as content filters.In one of our open-ended survey questions, we asked respondents for their opinions on what actions social media companies should take to make sure that their platforms are safe, civil places for public discussion (see Figure 6.1). Surprisingly, over a third of respondents were unsure (36%). This indicates a great need for public discussion about the options for platform self-regulation and the governance of public speech environments, as well as exploration of the ways in which social media companies can work with users to improve the experience of social interaction.

This chapter began by probing Australian attitudes to free speech as litmus test in understanding their appetite for greater communicative freedoms. One of its central findings is that Australians are strongly supportive of greater monitoring and regulation of online speech environments, as well as intervention by social media companies in content moderation and the removal of harmful speech. Our respondents were also in favour of greater user education for better understanding of speech rights and responsibilities. When our discussion group participants were asked whether online behaviour is currently less controllable by law or rules than offline behaviour, they agreed, arguing that more rules or

Figure 6.1 Opinions on social media self-regulation



guidelines need to be in place for people to learn 'what to share and what not to share' 'what can be seen and what can be written' and 'what people can post'. They also raised concerns about the creation of fake accounts, the way social media can be used to 'destroy people's lives' and the need to have 'more ability to remove what's posted'.

It seems, however, that very few participants were aware of the procedural difficulties of having content removed from social media sites, or of the fact that the major platforms are reluctant to take primary responsibility for moderating content and devote relatively few resources to monitoring and responding to complaints. These difficulties are well documented in the European Commission's 2016–17 attempts to have social media companies remove hate speech speedily on receipt of a formal complaint. Recent UK research into homophobic hate online has also shown that nearly half of those surveyed did not find it easy to report, and some of those who had contacted social media platforms had been deterred from taking further action after they received no response or an automated reply with no follow-up (Stray, 2017).[3] Thus, even though major companies like Microsoft are encouraging young people to report 'cruel, abusive and inappropriate content and conduct' (Microsoft, 2017), it is necessary to ensure that there are accountability mechanisms built into this drive. If Australians expect content reporting to be 'easy', government and relevant civil society organisations need to explore the roles they might play in making sure social media complaints processes are simple to negotiate, have clear, commensurate outcomes and are reported transparently. Similarly, there must be open avenues for appeal against platform sanctions for posting inappropriate content, such as account suspension.

In this study then we have identified a *perceptual gap* between what ordinary Australians think is the digital policy environment (it's easy to get content removed from online publications and platforms) and what is evident from public accounts of content removal struggles internationally (it is not easy, and takes time and negotiation). There is also a *normative gap* between what people think should be happening (social media platforms should monitor and proactively remove content) and what social media companies think are the limits of their responsibilities.

In legal and trade dealings with governments internationally, the major social media companies have maintained that they are technology businesses, which simply host services that enable their users to publish and network with each other (Napoli & Caplan, 2017). Our research indicates that Australians expect them to behave more like media companies, exerting control over the standard of content they host and working with government and users on improving the safety and civility of their communicative domains. The way in which we choose to move forward in law, policy and regulation of online speech, however, might better tend towards co-regulatory agreements than direct legal interventions, as the following case study suggests.

6.6 Hate speech: co-regulation for rights protection and education

The degree of responsibility that social media platforms should have for content moderation is a subject of intense debate, particularly in Europe. There, two contrasting regulatory moves are testing the possibilities for controlling hate speech against refugees in the wake of the 2015–16 immigration crisis. The first is a voluntary, cooperative agreement between the European Commission (EC) and the major social media platforms designed to reduce the incidence of hate speech through better complaints reporting and standards education. The other move is national legal intervention, with a new anti-hate speech law introduced in Germany, which will bind platforms to time-sensitive content takedowns.

The problem of online hate speech came to a head in Europe after an upswing in xenophobic, politically extremist and violent, racially discriminatory posts on social media channels, following the 2015–16 waves of refugees and economic migrants into southern Europe from Syria, Afghanistan, Iraq, North Africa and the Balkans. At the EC's first Annual Colloquium on Fundamental Rights, it observed that that '[h]ate speech, which incites to violence and hatred, particularly online, was identified as increasingly worrying, and now constituting the main source of hate incidents' (European Commission, 2015).[4] Participants noted the need to cooperate with social media platforms to combat hate speech, and to better record, act on and prosecute hate crimes. As an outcome, the EC committed to dialogue with 'IT companies', as well as businesses, national authorities and civil society on ways to tackle hate speech, including 'by making it easier for users to report illegal content to companies' (European Commission, 2015).

In March 2016, the European Commission announced its Code of Conduct On Countering Illegal Hate Speech Online, creating a non-binding framework for cooperation between the EC, EU Member States, civil society organisations (CSOs) and the four largest transnational technology companies to reduce and counter illegal hate speech narratives. As the code notes, the aim is to stop the proliferation of speech that 'not only negatively affects the groups or individuals that it targets, [but] … also negatively impacts those who speak out for freedom, tolerance and non-discrimination in our open societies and has a chilling effect on the democratic discourse on online platforms' (European Union, 2016b).

Aside from requiring the platforms to review and take down the majority of illegal speech within 24 hours, the Code also requires the platforms to work with CSOs and trusted reporters on clarifying reporting procedures and expediting expert notifications, as well as developing strategies to promote counter narratives. Finally, it encourages those companies to cooperate with other non-signatory social media services in sharing information about, and developing best practices in, the detection, reporting, review and removal of hate speech.

Progress on the agreement was not rapid. The first report in December 2016 showed that only 28% of notifications resulted in take-downs, and only 40% of notifications were processed within 24 hours, while another 43% took 48 hours (European Commission, 2016c). However, a second review in June 2017 suggested that companies had more than doubled their incidence of content removal to 59% and increased their review capacity. Two concerns were raised about platform responsiveness, however, with companies being less likely to remove content flagged by citizens rather than trusted reporters, and differing significantly in the quality of feedback they gave on moderation decision-making (European Commission, 2016b). EU Commissioner for Justice, Consumers and Equality Věra Jourová said that while the achievements were 'encouraging', she wanted to see 'the IT companies provide better feedback to those who notified cases' and make 'further progress to deliver on all the commitments' (European Commission, 2016d).

In contrast to this cooperative arrangement, Germany has just legislated, under its *Network Enforcement Act 2017*, or NetZDG, to force social media companies to take down illegal speech within 24 hours or face up to €50 million in fines.[5] The German approach, which has been championed by Justice Minister Heiko Maas, is consistent with the nation's hard line, following World War II, on constraining hate speech or *Volksverhetzung* – incitement of people. This concept is defined in paragraph 130 of the German Criminal Code as an act that:

- incites hatred against segments of the population or calls for violent or arbitrary measures against them, or
- assaults the human dignity of others by insulting, maliciously maligning, or defaming segments of the population.

The NetzDG, which came into force in October 2017, is wider in scope than the EC scheme in application and penalties. It applies to all profit-making internet platforms that enable users to share content with others or make it publicly available, and so could include gaming communities as well as social media. It requires services to 'remove or block obviously unlawful content within 24 hours of receipt of a complaint', while a second category of 'controversial content', which may or may not be illegal in Germany, must be reviewed and evaluated for removal within seven days. As critics have noted, the time limit may lead to over-enforcement to avoid penalties. It also puts US companies with

First Amendment-modelled community standards into potential conflict with administering German defamation and criminal insult laws (Lee 2017).

Both the German law and the European Code are distinct attempts by governments to shape the development of transnational and cross cultural speech standards that would otherwise be set by US-based private enterprise. The problem is that these measures contribute to the jurisdictional peculiarities that are creating a 'splinternet' of regulatory conditions for online communication.

The benefits of the EC approach are that it:

- mandates better definition and awareness of best practice reporting practices and complaints processing
- supports community and corporate education on illegal speech forms and impacts, and
- encourages cooperative strategies for reducing harmful behaviour and promoting counter-narratives to extremist speech.

Importantly, it potentially spreads the responsibility for reporting hateful and offensive speech from the individual to a network of expert reporting organisations, and introduces accountability measures to evaluate the success of the scheme – which may become self-regulatory in the future. For these reasons, this type of institutional support for individual speech rights and responsibilities appears a more equitable and flexible means of regulating for communicative change than relying on national legislation alone.

Endnotes

1 Highly publicised instances of cyberbullying have included that of television host Charlotte Dawson, prior to her suicide, and the trolling of former Primer Minister Julia Gillard (Morrissey & Yell, 2016). The latter case led Gillard to negotiate the 2013 'Cooperative Arrangement for Complaints Handling on Social Networking Sites' with Facebook, Google/ YouTube, Yahoo! And Microsoft (DBCDE, 2013).

2 Coalition MPs, for example, led the 2017 parliamentary move to reform section 18C of the *Racial Discrimination Act 1975*, which makes it illegal to offend, insult, humiliate or intimidate someone because of their race, colour, or national or ethnic origin.

3 In November 2017, the United Kingdom instituted new Crown Prosecution Service guidance for the handling of online hate speech cases by prosecutors and police, to try and improve prosecution rates.

4 This refers to hate speech as defined by the EC Framework Decision 2008/913/JHA of 28 November 2008.

5 Germany's *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* [Act to Improve the Enforcement of Rights on Social Networks] 2017 is popularly known as the *Netzwerksdurchsetzungsgesetz* (Network Enforcement Act) or NetzDG.

Bibliography

Adams, S., Purtova, N. & Leenes, R. (eds). (2017). *Under observation: The interplay between eHealth and surveillance*. Cham: Springer.

Aloisi, A. (2016). Commoditized workers: Case study research on labour law issues arising from a set of 'on demand/gig economy' platforms. *Comparative Labor Law & Policy Journal*, 37(3), 653–90.

Australian Computer Society (ACS). (2017). *Data sharing frameworks: Technical whitepaper*. September. Retrieved from https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Data-Sharing-Frameworks_FINAL_FA_SINGLE_LR.pdf.

Australian Government (2017). *Review of whether there should be exceptions to the prohibition on civil litigant access to retained telecommunications data*. Retrieved from https://www.ag.gov.au/Consultations/Documents/Access-to-telecommunications-data/Review-civil-litigant-access-to-retained-telecommunications-data.pdf.

Australian Law Reform Commission (ALRC) (2014). *Copyright and digital economy*. ALRC Report 122. Retrieved from https://www.alrc.gov.au/publications/copyright-report-122.

Australian Law Reform Commission (ALRC). (2014). *Serious invasions of privacy in the digital era*. Report No. 123.

Australian Law Reform Commission (ALRC). (2014). *Serious invasions of privacy in the digital era*. Sydney: ALRC. Retrieved from https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123.

Australian Productivity Commission (PC). (2017). Report 82: *Data Availability and Use*. Melbourne: PC.

Australian Public Service Commission (APSC). (2017). *Making public comment on social media: A guide for APS employees*. Canberra: ASPC. Retrieved from http://www.apsc.gov.au/publications-and-media/current-publications/making-public-comment.

Bartlett, J., Norrie, R., Patel, S., Rumpel, R. & Wibberley, S. (2014). *Misogyny on Twitter*. London: Demos. Retrieved from https://www.demos.co.uk/files/MISOGYNY_ON_TWITTER.pdf.

Bates, C., Imrie, R. & Kullman, K. (eds) (2016). *Care and design: Bodies, building, cities*. New York: Wiley-Blackwell.

Boys, J. (2014). *Doing design differently: An alternative handbook on architecture, dis/ability, and designing for everyday life*. Oxford: Routledge.

Brock, G. (2016). *The right to be forgotten: Privacy and the media in the digital age*. London: I.B. Tauris.

Bunz, M. & Meikle, G. (2017). *The internet of things*. Cambridge: Polity Press.Byrnes, A. (2009). *Bill of Rights in Australia: History, politics, and law*. Sydney: UNSW Press.

Campbell, T., Goldsworthy, J. & Stone, A. (eds). (2006). *Protecting rights without a Bill of Rights: Institutional performance and reform in Australia*. Aldershot: Ashgate.

Chappell, L., Chesterman, J. & Hill, L. (2009). *The politics of human rights in Australia*. Melbourne: Cambridge University Press.

Cohen, J. (2012). *Configuring the networked self: Law, code and the play of everyday practice*. New Haven, CT: Yale University Press.Cole, D., Fabbrini, F. & Schulhofer, S. (eds). (2017). *Surveillance, privacy, and transatlantic relations*. Oxford: Bloomsbury.

Community and Public Sector Union (CPSU). (2017). Submission to the APSC Review *Making public comment*. Retrieved from http://www.cpsu.org.au/system/files/cpsu_submission_to_making_public_comment_review.pdf.

Daly, A. (2016). 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. 128–36). Hong Kong: Digital Asia Hub. Retrieved from https://www.digitalasiahub.org/thegoodlife.

Daly, A. (2016). Net neutrality in Australia: The debate continues, but no policy In sight. In L. Belli & P. De Filippi (eds), *Net neutrality compendium: Human rights, free competition and the future of the internet* (pp. 141–56). Heidelberg: Springer.

Daly, A. (2017). Privacy in automation: An appraisal of the emerging Australian approach. *Computer Law & Security Review: The International Journal of Technology Law and Practice*. DOI: 10.1016/j.clsr.2017.05.009.

Department for Broadband, Communications and the Digital Economy (DBCDE). (2013). *Cooperative arrangement for complaints handling on social networking sites*. https://www.communications.gov.au/sites/g/files/net301/f/Cooperative_Arrangement_for_Complaints_Handling_on_Social_Networking_Sites.pdf.

Department of Communications and the Arts (2017). Civil penalties regime for non-consensual sharing of intimate images. Discussion paper. May 2017. Australian Government. Retrieved from https://www.communications.gov.au/have-your-say/civil-penalty-regime-non-consensual-sharing-intimate-images

De Stefano, V. (2016). *The rise of the 'just-in-time workforce': On-demand work, crowdwork and labour protection in the 'gig-economy'*. Conditions of work and employment series, no. 71. Geneva: Inclusive Labour Markets, Labour Relations and Working Conditions Branch, International Labour Office. Retrieved from http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_443267.pdf.

DeVito, M.A. (2017). From editors to algorithms: A values-based approach to understanding story selection in the Facebook news feed. *Digital Journalism*, 5(6), 753–73.

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

Eurofound and International Labour Office (ILO). (2017). *Working anytime, anywhere: The effects on the world of work*. Luxembourg: European Union and Geneva: ILO. DOI: 10.2806/372726.

European Commission (2015). Joining forces against antisemitic and antiMuslim hatred in the EU: outcomes of the first Annual Colloquium on Fundamental Rights. Brussels October 9 2015. Retrieved from http://ec.europa.eu/justice/events/colloquium-fundamental-rights-2015/files/fundamental_rights_colloquium_conclusions_en.pdf

European Commission (2016a) The European Digital Competence Framework for Citizens. Luxembourg: Publications Office of the European Union. Retrieved from http://ec.europa.eu/social/main.jsp?catId=1315&langId=en

European Commission (2016b) European Commission (2016a). Code Of Conduct On Countering Illegal Hate Speech Online. March 31 2016. Retrieved from http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

European Commission (2016c). *Code of Conduct on countering illegal hate speech online: First results on implementation*. Directorate-General for Justice and Consumers. Retrieved from http://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf.

European Commission (2016d). Countering online hate speech – Commission initiative with social media platforms and civil society shows progress. Press release, 1 June. Retrieved from http://europa.eu/rapid/press-release_IP-17-1471_en.htm.

European Union (EU). (2016). *Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1.

Executive Office of the President (2015). Big data and differential processing. White House, Washington, DC: Executive Office. Retrieved from http://1.usa.gov/1eNy7qR.

Facebook (Rob Goldman) (2017). Update on our advertising transparency and authenticity efforts. *Facebook Newsroom*, 27 October. Retrieved from https://newsroom.fb.com/news/2017/10/update-on-our-advertising-transparency-and-authenticity-efforts.

Fairfield, J. (2017). *Owned: Property, privacy, and the new digital serfdom*. Cambridge: Cambridge University Press.

Flecker, J. (ed.). (2016). *Space, place, and global digital work*. Basingstoke: Palgrave Macmillan.

Friedewald, M., Burgess, J. P., Čas, J., Bellanova, R. & Peissl, W. (eds). (2017). *Surveillance, privacy and security: Citizens' Perspectives*. London: Routledge.

Fuchs, C. (2014). *Digital labour and Karl Marx*. New York: Routledge.

Gahan, P., Healy, J. & Nicholson, D. (2017). Technology, the digital economy and the challenge for labour market regulation. In J. Howe, A. Chapman and I. Landau (eds), *The evolving project of labour law: Foundations, development, and future research directions*. Sydney: Federation Press.

Gaze, B. & Hunter, R. (2010). *Enforcing human rights in Australia: An evaluation of the new regime*. Sydney: Themis Press.

Gelber, K. (2011). *Speech matters: Getting free speech right*. Brisbane: University of Queensland Press.

Gerber, P. & Castan, M. (eds). (2013). *Contemporary perspectives on human rights law in Australia*. Sydney: Thomson Reuters.

Goh, B.C., Offord, B. & Garbutt, R. (eds). (2012). *Activating human rights and peace: Theories, practices, and contexts*. Aldershot: Ashgate.

Goldsworthy, T. (2017). Revenge porn laws may not be capturing the right people. *The Conversation*, 29 September. Retrieved from https://theconversation.com/revenge-porn-laws-may-not-be-capturing-the-right-people-84061.

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

Gregg, M. (2011). *Work's intimacy*. Cambridge: Polity Press.

Gutwirth, S., Leenes, R., de Hert, P. & Poullet, Y. (eds) . *European data protection: Coming of age*. Dordrecht: Springer.

Henry, N., Powell, A. & Flynn, A. (2017). *Not just 'revenge pornography': Australians' experiences of image-based abuse*. Melbourne: Centre for Global Research & Centre for Applied Social Research, RMIT University. Retrieved from https://www.rmit.edu.au/content/dam/rmit/documents/college-of-design-and-social-context/schools/global-urban-and-social-studies/revenge_porn_report_2017.pdf.

Hunt, L. (2007). *Inventing human rights: A history*. New York: W.W. Norton.

Jaffe, E.M. (2016). Swatting: The new cyberbullying frontier after *Elonis v. United States*. *Drake Law Review*, *64*, 455–83.

Karppinen, K (2017) Deconstructing Digital Rights: Promises and Problems of Rights-Based Politics. Paper presented at the Nordmedia 2017 conference, Political communication division Tampere 17-19 August 2017.

Katz, I., Keeley, M., Spears, B., Taddeo, C., Swirski, T. & Bates, S. (2014). *Research on youth exposure to, and management of, cyberbullying incidents in Australia*. Social Policy Research Centre, University of South Australia, University of Western Sydney, and Young and Well Cooperative Research Centre. June. Canberra: Department of Communications. Retrieved from https://www.communications.gov.au/departmental-news/cyberbullying-research-report.

Karpinnen, K. (2017). Deconstructing digital rights: Promises and problems of rights-based politics. Paper presented at the Nordmedia 2017 conference, Political communication division, Tampere, August, 17-19. Retrieved from https://www.researchgate.net/publication/319877470.

Laidlaw, E.B. (2015). *Regulating speech in cyberspace: Gatekeepers, human rights, and corporate responsibility*. Cambridge: Cambridge University Press.

Lam, H. (2016). Social media dilemmas in the employment context. *Employee Relations*, 38(3), 420–37.

Lee, D. (2017). Germany's NetzDG and the threat to online free speech. *Case Disclosed*, 10 October. Media Freedom and Information Access Clinic. Yale Law School. Retrieved from https://law.yale.edu/mfia/case-disclosed/germanys-netzdg-and-threat-online-free-speech.

Leonard, P. (2016). *Mandatory internet data retention in Australia: Evidentiary uses and challenges*. Sydney: Gilbert & Tobin. Retrieved from https://www.gtlaw.com.au/mandatory-internet-data-retention-australia-%E2%80%93-looking-horse-mouth-after-it-has-bolted.Leonard, P. (2017). Emerging concerns for responsible data analytics: Trust, fairness, transparency, and discrimination. Paper for the NSW Data Analytics Centre Showcase, 12 July. Retrieved from http://www.commsalliance.com.au/__data/assets/pdf_file/0018/58104/Peter-Leonard-Emerging-Concerns-for-Responsible-Data-Analytics_-Trust-Fairness-Transparency-and-Discrimination-Paper-for-the-NSW-Data-Analytics-Centre-Showcase-12-Jul.pdf.

Lessig, L. (2004). *Free culture: How big media uses technology and the law to lock down culture and control creativity*. New York: Penguin.

Lessig, L. (2008). *Remix: Making art and commerce thrive in the hybrid economy*. New York: Penguin.

Lewchuk, W. (2017). Precarious jobs: Where are they, and how do they affect well-being? *The Economic and Labour Relations Review,* 28(3), 402–19.

Livingstone, S. & Third, A. (2017). Children and young people's rights in the digital age: an emerging agenda. New Media & Society, 19, 5, 657-670.

Lloyd, J. (2017). Media statement on social media guidance, 7 August. Retrieved from http://www.apsc.gov.au/home/news-and-events/social-media.

Martin, C. (2016). The sharing economy: A pathway to sustainability or a nightmarish form of neoliberal capitalism? *Ecological Economics*, *121*, 149–59.

Marwick, A.E. & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–67.

McDonald, P. & Thompson, P. (2016). Social media(tion) and the reshaping of public/private boundaries in employment relations. *International Journal of Management Reviews, 18*(1), 69–84.

Méda, D. & Vendramin, P. (2017). *Reinventing work in Europe: Value, generations, and labour*. Basingstoke: Palgrave Macmillan.

Meil, P. & Kirov, V. (eds) (2017). *Policy implications of virtual work*. Basingstoke: Palgrave Macmillan.

Mettler, K. & Selk, A. (2017). GoDaddy – then Google – ban neo-Nazi site *Daily Stormer* for disparaging Charlottesville victim. *Washington Post*, 14 August. Retrieved from https://www.washingtonpost.com/news/morning-mix/wp/2017/08/14/godaddy-bans-neo-nazi-site-daily-stormer-for-disparaging-woman-killed-at-charlottesville-rally/?utm_term=.bf6f95a48e81.

Microsoft. (2017). *Digital Civility Index (DCI) – International 2017*. February. Telecommunication Research Group for Microsoft Corporation. Retrieved from https://blogs.microsoft.com/on-the-issues/2017/02/07/microsoft-releases-digital-civility-index-challenges-people-empathetic-online.

Morgan, R. (2017). Australians not concerned about use of mass facial recognition technology. Media release, 10 October. Retrieved from https://www.roymorgan.com/findings/7366-roy-morgan-snap-sms-survey-facial-recognition-surveillance-technology-october-10-2017-201710101059.

Morrissey, B. & Yell, S. (2016) Performative trolling: Szubanski, Gillard, Dawson and the nature of the utterance. *Persona Studies,* 2(1), 27–40.

Moyn, S. (2010). *The last utopia: Human rights in history*. Cambridge, MA: Harvard University Press.

Napoli, P. & Caplan R. (2017). Why media companies insist they're not media companies, why they're wrong, and why it matters. *First Monday*, 22(5), 1–13.

Nissenbaum, H. (2010) *Privacy in context: Technology, policy, and the integrity of social life.* Stanford, CA: Stanford University Press.

Norris, C., de Hert, P., L'Hoiry, X. & Galleta, A. (eds). (2017). *The unaccountable state of surveillance: Exercising access rights in Europe*. Cham: Springer.
OECD. (2016a). *The future of work: Digitalisation in the US labour market*. Compilation of briefings for the EMPL committee. Retrieved from http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/578959/IPOL_BRI(2016)578959_EN.pdf.

OECD. (2016b). *New forms of work in the digital economy.* 2016 Ministerial meeting on the digital economy: Technical report. Paris: OECD. Retrieved from http://dx.doi.org.ezproxy1.library.usyd.edu.au/10.1787/5jlwnklt820x-en.

OECD. (2017). *Digital economy outlook*. Paris: OECD.

OFCOM. (2016). Adults' media use and attitudes report 2016. London: OFCOM. Retrieved form https://www.ofcom.org.uk/__data/assets/pdf_file/0026/68930/mla-questionnaire.pdf.

Office of the Children's eSafety Commissioner (2016). Submission on the 'Phenomenon colloquially referred to as "revenge porn", which involves sharing private sexual images and recordings of a person without their consent, with the intention to cause that person harm.' Submission 22. Senate Legal and Constitutional Affairs References Committee Inquiry. Retrieved from https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Revenge_porn/Submissions.

Office of the eSafety Commissioner (2017). Image based abuse: Pathways and prevalence. October. Retrieved from https://esafety.gov.au/image-based-abuse/about/research/prevalence-pathways-text.

Ohler, J. (2010). Digital Community, Digital Citizen. Thousand Oaks: Corwin/Sage.

Pasquale, F. (2015). *Blackbox society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.

Pew Research Centre. (2016, November 17). Gig work, online selling and home sharing. Washington, D.C.: Pew. Retrieved from http://www.pewinternet.org/2016/11/17/gig-work-online-selling-and-home-sharing/0.

Pew Research Center. (2015, November 18). Global support for principle of free expression, but opposition to some forms of speech. Washington, D.C.: Pew. Retrieved from http://www.pewglobal.org/2015/11/18/global-support-for-principle-of-free-expression-but-opposition-to-some-forms-of-speech/.

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

Pew Research Centre. (2016, March 10). Public predictions for the future of workforce automation. Washington, DC: Pew. Retrieved from http://www.pewinternet.org/2016/03/10/public-predictions-for-the-future-of-workforce-automation/.

Pew Research Centre. (2014, August 26). Social media and the "spiral of silence." Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/2014/08/26/social-media-and-the-spiral-of-silence/.

Pew Research Centre. (2013, December 30). Social media update 2013. Pew Research Center, Washington, D.C.: Pew. Retrieved from http://www.pewinternet.org/2013/12/30/social-media-update-2013/.

Pew Research Centre. (2015, June 22). Social media and the workplace. Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/2016/06/22/social-media-and-the-workplace/0.

Powell, A. & Henry, N. (2015). Digital Harassment and Abuse of Adult Australians: A summary report. Melbourne: RMIT University. https://research.techandme.com.au/wp-content/uploads/REPORT_AustraliansExperiencesofDigitalHarassmentandAbuse.pdf.

Productivity Commission (PC). (2016). *Digital disruption: What do governments need to do?* Melbourne: PC. Retrieved from https://www.pc.gov.au/research/completed/digital-disruption.

Riley, J. (2017). *Regulating work in the 'gig economy'*. In M. Roennmar & J.J. Votinius (eds), *Festskrift Till Ann Numhauser*-Henning (pp. 669–84). Juristfoerlaget i Lund, Sweden. Sydney Law School Research Paper No. 17/30. Retrieved from https://ssrn.com/abstract=2949631.

Ruby, F., Goggin, G. & Keane, J. (2017). 'Comparative silence' still? Journalism, academia, and the five eyes of Edward Snowden. *Digital Journalism*, 5(3), 353–67.

Senate Community Affairs Reference Committee (Senate). (2017). *Design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System initiative*. Canberra: Commonwealth of Australia. Retrieved from https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Community_Affairs/SocialWelfareSystem/Report.

Steppe, R. (2017). Online price discrimination and personal data: A General Data Protection Regulation perspective. *Computer Security and Law Review*, 33(6), 768–85.

Stewart, A. & Stanford J. (2017). Regulating work in the gig economy: What are the options? *The Economic and Labour Relations Review*, 28(3), 420–37.

Stray, M. (2017). *Online hate crime report 2017: Challenging online homophobia, biphobia and transphobia*. London: Galop.org.uk. Retrieved from http://www.galop.org.uk/wp-content/uploads/2017/08/Online-hate-report.pdf.

Taylor, E. & Rooney, T. (eds) (2016). *Surveillance, childhood and youth*. Oxford: Routledge.

Thornthwaite, L. (2013). Chilling times: Labour law and the regulation of social media policies. Paper presented to Labour Law Research Network Inaugural Conference, Barcelona, June. Retrieved from https://www.upf.edu/documents/3298481/3410076/2013-LLRNConf_Thornthwaite.pdf/da1a688a-caea-4c70-9bb4-adf4ea35c42e.

Tufecki, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colorado Technology Law Journal*, 13, 203–17.

University of Southern California Annenberg School Center for the Digital Future. (2016). The Digital future report. Retrieved from http://www.digitalcenter.org/wp-content/uploads/2013/10/2017-Digital-Future-Report.pdf.

Verhulst, S.G., Price, M.E. & Morgan, E. (eds). (2013). *Routledge handbook of media law.* Oxford: Routledge.

Vromen, A. (2017). Digital Citizenship and Political Engagement: The Challenge from Online Campaigning and Advocacy Organisations. London: Palgrave Macmillan

Wacks, R. (1980). The poverty of privacy. *Law Quarterly Review*, 96, 73–95.

Williams, G. (2004). *The case for an Australian Bill of Rights*. Sydney: UNSW Press.

Williams, G. (2007). *A charter of rights for Australia.* Sydney: UNSW Press.

Williams, G. & Hume, D. (2013). *Human rights under the Australian Constitution* (2nd ed.). Melbourne: Oxford University Press.Wilson, J.A. & Yochim, E.C. (2017). *Mothering through precarity: Women's work and digital media*. Durham, NC: Duke University Press.

Yeung, K. (2017). Algorithmic regulation: A critical Interrogation. *Regulation and Governance*. DOI: 10.1111/rego.12158.

Appendix

Digital Rights Survey: Essential Media Script and Questionnaire

Introduction

Thank you for agreeing to participate in this survey. We want to talk to you today about rights and responsibilities in using the internet and social media. We'd like to get opinions about information privacy, work, and how people talk online. There are no right or wrong answers, we are interested in how you think about these questions.

The survey is for research purposes only, and we would like to remind you that your answers are anonymous and confidential. Your responses will not be attributed to you directly.

This survey will take around 15 minutes to complete.

Section 1: Background [ask both waves]

QA: Which of these best describes what you were doing for most of last week:

a. In full-time paid work (or away temporarily, e.g. on holidays or sick leave)
b. In part-time/casual paid work (or away temporarily, e.g. on holidays or sick leave)
c. Looking after your own children / the home
d. Retired
e. Otherwise not in paid work

[Ask QB if QA = A or B]

QB: If working: Which of the following best describes your current occupation?

a. (Professional/Managerial
b. Sales/Clerical
c. Technical/Skilled
d. Manual work/Labourer
e. Other (please specify).

QC: Are you the parent or guardian of any children under age 18 now living in your household?

- Yes
- No

Q1: Which of the following devices do you use to connect to the internet? [Multiple response]

a. Desktop or laptop computer
b. Mobile phone
c. Tablet
d. E-reader
e. Web browser connected to your TV (e.g. through a Kodi box)

Q2: Please rank the following from the devices you use most often to connect to the internet to the devices you use least [for all devices used at Q1]

a. Desktop or laptop computer
b. Mobile phone
c. Tablet
d. E-reader
e. Web browser connected to your TV (e.g. through a Kodi box)

[Ask if use 'mobile phone' at Q1]

Q3: Excluding those that came preinstalled, how many additional apps do you have installed on your mobile phone?

a. Less than 5
b. 5-10
c. 11-20
d. More than 20

Q4: Which of the following social media services do you use:

[Multiple response A-F, if G chosen must be only option]

a. Facebook
b. Twitter
c. Instagram
d. Snapchat
e. WeChat
f. Weibo
g. None of the above

[Ask Q5 if more than one option chosen at Q4]

Q5: Which of those do you use most often?

[List only options chosen at Q4]

a. Facebook
b. Twitter
c. Instagram
d. Snapchat
e. WeChat
f. Weibo

[Ask for the option selected in Q5]

Q6. For [social media platform], please specify how often you do each of the following?[1]

		Several times a day	Once a day	3-5 days a week	1-2 days a week	Every few weeks	Less often	Never
A	Post a comment or image							
B	Like or favourite other people's posts, photos, or links							
C	Comment on other people's posts, photos, or links							
D	Share or retweet other people's posts, photos, or links							
E	Send private messages							

Q7. What do you think are the most important political, social or legal issues with the internet and digital technologies that need to be addressed in the next five years or so? [Open-ended]

Q8. What steps if any do you think social media companies should take to ensure their platforms are safe, civil spaces for public discussion?

Section 2: Information/Privacy [ask both waves]

Q9: Please indicate how strongly you agree or disagree with the following statements[2]:

		Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Unsure
A	I want to know what social media companies do with the information they collect, share, keep and use about me						
B	Media companies are entitled to republish material they find on people's social media accounts as it has already been publicly shared with others						
C	The internet needs to be regulated in terms of what can be shown and written online						
D	[If use any social media service at Q4] I have a good understanding of how to adjust my privacy settings on social media sites						

Q10: Do you believe the following are breaches of your privacy?:

		Definitely a breach of my privacy	Sort of a breach of my privacy	Not really a breach of my privacy	Definitely not a breach of my privacy	Unsure
A	If the government requires my phone company to keep information about who I call and when					
B	If a prospective employer looks at my **public** social media profile					
C	If someone in my social network publishes online a photo of me without my permission					

Q11: How strongly do you agree or disagree with the following?[3]

		Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Unsure
A	I actively protect my privacy online						
B	I have nothing to hide						
C	I feel I can control my privacy online						
E	There is no privacy – get over it						
F	Concerns about privacy online are exaggerated						
G	I am concerned corporations are violating my privacy online						
H	I am concerned governments are violating my privacy online						
I	I am concerned other people are violating my privacy online						

Q12: If you could access reports on the internet user profiles constructed about you, how important would it be for you to know about the following:

		Very important	Important	Somewhat important	Not at all important	Unsure
A	Records of what you have bought online					
B	Records of what you have done on social media					
C	The list of third party companies that can access your profile					
D	What third party companies do with your personal information					
E	How to report or correct inaccurate information					

Q13: Have you ever had your privacy violated online? How did it affect you? Choose all that apply[4]

[Multiple response apart from A]

a. No
b. Yes and it affected my personal relationships
c. Yes and affected my job / career
d. Yes and it had financial consequences
e. Yes and it was embarrassing
f. Yes and it was a minor problem

Q14: Have you ever used any of the following?

		Yes, for work	Yes, for other reasons	Yes, for both work and other reasons	No	Unsure
A	A virtual private network (VPN)					
B	Encrypted messaging or encrypted email					
C	An internet privacy tool such as TOR					

[Ask if use any social media services at Q4]

Q15: Thinking specifically about the social media platform you use most often, have you changed the privacy settings from the original default setting to restrict who can access your profile? [5]

a. Yes

b. No

c. Unsure

Q16: In making decisions about what information to share with companies online, at any point in the last month have you felt any of the following? (tick box for those that apply)[6]

[Multiple response]

a. Discouraged by the amount of effort needed to understand what would be done with your data

b. Confused by the information provided in a privacy policy

c. Confident that you understood what would be done with your data

d. Impatient because you wanted to learn more but needed to make a decision right away

Q17: Should the government be able to prevent media organisations from publishing information about the following? [7]

		Media should always be allowed to publish	Media should be allowed to publish in some circumstances	Government should be able to prevent media from publishing	Unsure
A	Large political protests in our country				
B	Economic issues that might destabilise the country's economy				
C	Sensitive issues related to national security and foreign relations				

Q18: Do you FAVOUR or OPPOSE the following[8]

		Strongly favour	Somewhat favour	Somewhat oppose	Strongly oppose	Unsure
A	A government program to collect communications of nearly all internet users as part of anti-terrorism efforts					
B	The government requiring internet service providers to store information about who you contact, when, and what websites you visit					
C	Law enforcement and security agencies being able to access information about who you contact, when, and what websites you visit					
D	A government program that tracks your use of public services and benefits					

Section 3: Work [ask wave 1 only]

Q19: On a typical day, how much would you say you use the internet to do work-related tasks? [9]

a. Frequently

b. Sometimes

c. Hardly ever

d. Never

Q20: Which of the following does your workplace have?[10]

[Multiple response]

a. Policies or rules about how you present yourself on the internet, for example, what you can post on blogs and websites, or what information you can share about yourself online

b. Policies or rules about using social media while at work

Q21. How strongly do you agree or disagree with each of the following[11]

		Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Unsure
A	Social media distracts me from the work I need to do						
B	Social media lets me see too much information about my co-workers						
C	Social media is important for helping me do my work or job						
E	It is acceptable for prospective employers to look at your **public** social media posts						
F	It is acceptable for prospective employers to look at your **private** social media posts						
G	It is acceptable for current employers to look at your **public** social media posts						
H	It is acceptable for current employers to look at your **private** social media posts						

Q22: Do you ever do any of the following things?[12]

		Yes I have done this	Heard of it but not done it	Never heard of this before
A	Hire someone online to do a task or household errand, using a service like Airtasker			
B	Use driver services such as Uber			
C	Order food or alcohol home delivery using an online app such as Foodora or Deliveroo			

Q23: In recent years, technology has allowed individual workers to perform one-off tasks for people who need those services. Some people refer to this as "gig work". These workers typically do not follow a set schedule, and get paid as they pick up assignments instead of receiving an hourly wage or salary. Based on what you know, do you think these jobs…[13]

		Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Unsure
A	Are a good entry level job for people who are entering the workforce						
B	Leave workers financially insecure						
C	Are great for people who want a flexible schedule						
E	Are the kind of jobs you can build a career out of						
F	Are a good option for older people who don't want to work fulltime any more						

Q24: Which ONE of the following statements about government regulation of any of these online gig work platforms do you agree with most?

[Single response]

a. these platforms should be fully regulated to give gig workers the same kind of rights that other employees have

b. new employment-related regulations should be created specifically for these platforms

c. the relationship between these platforms and gig workers does not need to be regulated

d. not sure

Q25: How much have you heard about the debate happening in some cities over whether services like Uber should be regulated in the same way as existing taxi companies?

a. A lot

b. A little

c. Nothing at all

[Ask if QA = A or B (in paid work)]

Q26: How concerned are you about the following: [14]

		Very concerned	Somewhat concerned	Not too concerned	Not concerned at all	Unsure
A	Losing your job because your employer finds someone who is willing to do your job for less money					
B	Losing your job because you aren't able to keep up with the technical skills required to do it					
C	Losing your job because your employer uses machines or computer programs to replace human workers					
D	Losing your job or missing a job opportunity because of material posted by, or about, you on social media					

Section 4: Free speech
[ask wave 2 only]

Q27: How strongly do you agree or disagree with the following statements[15]

		Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Unsure
A	I should be free to say and do what I want online						
B	Everyone should be free to say and do what they want online						
C	Everyone should have the right to anonymity online						

Q28: How strongly do you agree or disagree that people should be able to make the following types of statements online[16]

		Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Unsure
A	Criticisms of government policies						
B	Criticisms of religious organisations or religious beliefs						
C	Criticisms of minority groups						
D	Sexually explicit statements						
E	Calls for violent protests						
F	Encouraging non-violent actions that break laws the person believes are wrong						

Q29: How important is it that social media platforms remove the following types of information as soon as possible (e.g. within 24 hours)?

		Very important	Important	Somewhat important	Not at all important	Unsure
A	Abuse targeted at an individual					
B	Sexual harassment					
C	Sexually explicit talk					
D	Hate speech that encourages violence					
E	Anti-government talk					
F	Extremist political talk					

Q30: Most social media companies and some governments demand people always use their real names when posting online. In the following situations, if you could use remain anonymous would you be likely to:

		More likely	Less likely	No difference	Unsure
A	Post honest and open views on the news				
B	Talk about sensitive topics like sexuality				
C	Pretend to hold views that you don't for amusement				
D	Question others' opinions				
E	Get into an argument with someone				

Q31: Which of the following have affected your online interactions?

[Multiple response]

a. Mean or abusive remarks
b. Trolling, harassment or bullying (sustained abuse)
c. Unwanted sexual contact (sexts, solicitation)
d. Violent sexual contact (revenge porn, sexualised threats)
e. Racism
f. Personal information exposed deliberately or maliciously (doxing)
g. Personal information posted without permission by others (eg. childrens' photos)
h. Impersonation or swatting (hoax calls made in your name)

Q32: Many websites and apps have a function to report things you find inappropriate or offensive. Which of the following apply to you:

a. I'm aware of this function and have used it in the last 12 months
b. I'm aware of this function but haven't used it in the last 12 months
c. I'm not aware of this function

[Ask if Q32 = a]

Q33: When you reported something, how satisfied were you with the response? If you've reported something more than once, please think of the most recent time you did it.

a. Very satisfied
b. Fairly satisfied
c. Fairly dissatisfied
d. Very dissatisfied

[Ask if use social media at Q4]

Q34: Has anything you've posted on social media ever been removed, censored or restricted?

a. Yes
b. No
c. Unsure

[Ask if Q34 = yes]

Q35: How clear are you about why the content was removed, censored or restricted?

a. Very clear
b. Fairly clear
c. Not particularly clear
d. Not at all clear

[Ask if Q34 = yes]

Q36: Have you ever tried to appeal or complain about a decision to remove your content?

a. Yes
b. No
c. Unsure

[Ask if Q36 = yes]

Q37: Were you satisfied with the response to your complaint?

a. Yes
b. No
c. Unsure

Q38: Which of the following have you ever done:

		Done this more than once	Done this once	Not done this
A	Reduced your own comments on social media due to other people's behaviour			
B	[if QC = Yes] Advised your child to reduce their social media use due to other people's behaviour			
C	Deleted one of your social media accounts due to abuse or bullying			
D	[if QC = Yes] Advised your child to delete an account due to abuse or bullying			

Section 5: Demographics [ask both waves]

a. Regardless of which party you intend to vote for or how you currently feel about the parties and their leaders, to which party do you generally feel closest?:

b. [Labor, Liberal, National, Greens, One Nation, Independent or Other Party, Don't Know, None of them]

c. Age groups (18-29, 30-39, 40-49, 50-59, 60-69, 70+)

d. Gender [M, F, other]

e. Location: [a capital city, a regional city, a small town, or a rural area.]

f. What is the highest level of education you have **completed**? [Did not complete high school, Completed high school, Skilled/vocational TAFE qualification, Bachelor degree or associate diploma, Masters or Higher post graduate qualification]

g. Do you speak a language other than English at home? If yes, which one: [Italian, Greek, Arabic, Cantonese/ Mandarin, Vietnamese, other (specify)]

h. Do you receive a disability pension or the disability support pension? (yes, no)

Thank you for taking our survey.

We will be running some **online discussion groups** in the next month or so. Would you mind if we perhaps re-contacted you later, to see if you're interested? You'd be under **no obligation** – you could decide at the time. You would receive **$100 to thank you**, if you participate in the group. (Please note: We never send advertising or try to sell anything. We only conduct genuine research.)

Yes, you may re-contact me about the online discussion group	1	CONTINUE
No, do not re-contact me	0	FINISH SURVEY

If yes: Great! Please provide some contact details so we can get in touch with you:

Full name	
Email address	
(Confirm email address)	

Endnotes:

1 Adapted from: "Social Media Update 2013", Pew Research Center, Washington, D.C. (December 30, 2013); http://www.pewinternet.org/2013/12/30/social-media-update-2013/

2 Adapted from: "Adults' media use and attitudes report 2016", OFCOM; https://www.ofcom.org.uk/__data/assets/pdf_file/0026/68930/mla-questionnaire.pdf)

3 "The Digital Future Report, 2016", University of Southern California Annenberg School Center for the Digital Future; http://www.digitalcenter.org/wp-content/uploads/2013/10/2017-Digital-Future-Report.pdf)

4 "The Digital Future Report, 2016", University of Southern California Annenberg School Center for the Digital Future; http://www.digitalcenter.org/wp-content/uploads/2013/10/2017-Digital-Future-Report.pdf)

5 Adapted from: "Adults' media use and attitudes report 2016", OFCOM; https://www.ofcom.org.uk/__data/assets/pdf_file/0026/68930/mla-questionnaire.pdf).

6 Adapted from: "Privacy and Information Sharing", Pew Research Center, Washington, D.C. (January 14, 2016); http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/

7 Adapted from: "Global Support for Principle of Free Expression, but Opposition to Some Forms of Speech", Pew Research Center, Washington, D.C. (November 18, 2015); http://www.pewglobal.org/2015/11/18/global-support-for-principle-of-free-expression-but-opposition-to-some-forms-of-speech/)

8 "Social Media and the 'Spiral of Silence'", Pew Research Center, Washington, D.C. (August 26, 2014); http://www.pewinternet.org/2014/08/26/social-media-and-the-spiral-of-silence/)

9 "Social Media and the Workplace", Pew Research Center, Washington, D.C. (22 June, 2015); http://www.pewinternet.org/2016/06/22/social-media-and-the-workplace/0

10 "Social Media and the Workplace", Pew Research Center, Washington, D.C. (22 June, 2015); http://www.pewinternet.org/2016/06/22/social-media-and-the-workplace/0

11 Adapted from: "Social Media and the Workplace", Pew Research Center, Washington, D.C. (22 June, 2015); http://www.pewinternet.org/2016/06/22/social-media-and-the-workplace/0

12 Adapted from: "Gig work, Online Selling and Home Sharing", Pew Research Center, Washington, D.C. (17 November, 2016); http://www.pewinternet.org/2016/11/17/gig-work-online-selling-and-home-sharing/0

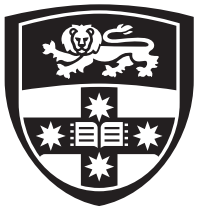
13 Adapted from: ""Gig work, Online Selling and Home Sharing", Pew Research Center, Washington, D.C. (17 November, 2016); http://www.pewinternet.org/2016/11/17/gig-work-online-selling-and-home-sharing/0

14 Adapted from: "Public Predictions for the Future of Workforce Automation", Pew Research Center, Washington, D.C. (10 March, 2016); http://www.pewinternet.org/2016/03/10/public-predictions-for-the-future-of-workforce-automation/

15 Adapted from: "Adults' media use and attitudes report 2016", OFCOM; https://www.ofcom.org.uk/__data/assets/pdf_file/0026/68930/mla-questionnaire.pdf.

16 Adapted from: "Global Support for Principle of Free Expression, but Opposition to Some Forms of Speech", Pew Research Center, Washington, D.C. (November 18, 2015); http://www.pewglobal.org/2015/11/18/global-support-for-principle-of-free-expression-but-opposition-to-some-forms-of-speech/

Australians are some of the world's greatest users of social media and mobile broadband, and the nation is in the top ten globally for internet use. At a time when use of these technologies is increasingly redefining aspects of personal and professional lives, Digital Rights in Australia explores urgent questions about the nature of our rights now and into the future. The analysis covers rights issues in four areas: privacy, profiling and analytics; government data-matching and surveillance; workplace change; and freedom of expression and speech regulation. It explores the ethical and legal challenges we face in using digital, networked technologies and the debates we are having about how to best manage their transformative impacts. Crucially this study examines the major role of private, transnational digital platforms in reshaping the way we work, study and conduct business, our interactions with government and with each other.



THE UNIVERSITY OF
SYDNEY