Submission to Human Rights and Technology Issues Paper

Nicolas Suzor,[1] Kim Weatherall,[2] Angela Daly,[3] Ariadne Vromen,[4] Monique Mann[5]

Executive Summary

We are a group of Australian academic researchers working in digital rights issues and the social implications and regulation of technology.

We welcome this consultation process and the ongoing participation of the AHRC in these debates. We believe that the AHRC is uniquely placed to contribute an important and distinct rights-oriented perspective to the many ongoing and intersecting debates about the development and deployment of new technologies in Australia. To date, this perspective has been under-represented in Australian policy debates, which have more often focused on innovation and ensuring that Australians benefit from new technologies.[6] It has also not been sufficiently represented in industry-led discussions about the ethical development and deployment of technology, which often proceed without a highly sophisticated understanding of human rights issues.

This submission focuses on a number of core issues that we suggest are key priorities or believe have been under-explored in public policy discussions to date. In particular, we:

- Urge the Commission to prioritise the role of enforceable laws backed by real sanctions in protecting human rights in Australia;
- Suggest that the Commission may play a very useful role in providing guidance and risk management frameworks for the development and deployment of new technologies to both private industry and public agencies;
- Provide a brief perspective on what we see as a principled approach for working through difficult questions of when legal liability should accrue and what role co-regulatory schemes should play in protecting human rights in technology;
- Recommend that the Commission recognise the ongoing problems that arise from the lack of an enforceable personal privacy right in Australia;
- Emphasise the importance of dealing with pressing structural inequalities in Australian technology and telecommunications policy, in guidance provided to industry and public agencies, and through appropriate legal obligations.

---

[1] QUT School of Law and Digital Media Research Centre, [redacted]

[2] University of Sydney Law School, [redacted]

[3] Chinese University of Hong Kong Faculty of Law, [redacted]

[4] University of Sydney, Department of Government and International Relations, Faculty of Arts and Social Sciences, [redacted]

[5] QUT School of Justice, [redacted]

[6] See for example Australian Productivity Commission, *Data Availability and Use* (Inquiry Report, March 2017)

The roles that this AHRC Inquiry can play

We think it is vitally important that rights-oriented perspectives are better integrated into policy and technical development in Australia. It is crucial, we suggest, that these ongoing debates and processes recognise more clearly that (a) there are distinct rights claims of human beings, arising from our inherent dignity, autonomy, integrity; (b) there are inalienable baseline entitlements that are non-negotiable; and (c) there are important obligations - for individuals, private sector and public sector - that accompany the recognition that human beings are entitled to respect and are not a 'means to an end'. These perspectives are particularly critical in the ongoing development of new technologies. Amid a discussion of new technologies in Australia that is often focused on the potential broad economic and social benefits of innovation, the human rights perspective can draw attention to the risk of subsuming inalienable individual rights in pursuit of the collective interest in policy-making, and - in the context of new technologies based on large-scale data analytics - the potential to lose sight of the fundamental dignity of human beings when datasets flow far beyond the initial point of collection, treating human beings as data points rather than individuals.

The existence of this inquiry has already catalysed discussion of these issues in Australia, and importantly, some discussion across disciplines and professions. Beyond this catalysing role, we think that there are a number of critical questions that this inquiry by the AHRC can address as steps towards better incorporating human rights perspectives into policy and technology development in Australia.

First, the AHRC can identify, investigate and document specific existing and imminent threats to human rights arising from current developments in technology. The Issues Paper already recognises a range of current and emerging threats posed by the rapid development of large-scale data analytics, machine learning, and automated decision-making. More specific examples have been identified in submissions and discussions catalysed by the inquiry. A great deal of attention in these areas has been paid to privacy and freedom of expression in particular, as well, more recently, as the right to be free from discrimination.[7] Other rights have been less systematically examined. It is important, we suggest, that more work be undertaken to provide guidance about a range of other risks, including:

- Implications of pervasive digitisation on labour rights[8] and Indigenous rights;[9]

---

[7] See eg Cathy O'Neill, 2016. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing.

[8] Consider, for example, the difficult questions at the intersection of privacy, freedom of association and freedom of speech that arise for employees when apparently 'private' communications on social media are seen as a threat to corporate reputation: see eg Goggin, G; Vromen, A, Weatherall, K, Martin, F, Webb, A, Sunman, L, Francesco, B, *Digital Rights in Australia* (2017), available at https://ses.library.usyd.edu.au/handle/2123/17587

[9] Kukutai, T and Taylor, J. (eds) *Indigenous Data Sovereignty: Towards an Agenda* (2016) ANU Press; Daly, Angela and Carlson, Anna and Van Geelen, Tess, Data and Fundamental Rights (February 7, 2018) in Vanessa Mak, Eric Tjong Tjin Tai and Anna Berlee (eds), Research Handbook on Data Science and Law (Edward Elgar, 2018, Forthcoming). Available at SSRN: https://ssrn.com/abstract=3072106 or http://dx.doi.org/10.2139/ssrn.3072106

- Fundamental issues of access and inclusion that are working to limit the participation of marginalised groups;[10] and
- The major risks of technologies working to amplify and reinforce existing structural inequalities in ways that are often opaque.

The AHRC can and should, through the collation of submissions, by talking to industry, academia and research bodies; to civil society and to members of the public, create an important record of, and analysis of, how the human rights of Australians are being impacted and will likely be impacted (positively and negatively) by developments in technology. Without that evidence base, recorded with the care, rigour and independence that are hallmarks of the work of an independent Human Rights Commission, it is more difficult for Australians to understand the implications of current developments, to demand better protection from policymakers and regulators, and where appropriate, to seek redress.

As part of this process of investigation, we would encourage the AHRC to use established human rights frameworks and methods to engage in a detailed way too with the tradeoffs between different rights (and other interests) involved in deploying new technologies. Both public sector agencies and industry could benefit from guidance on how to translate existing domestic and international legal obligations into informed policy and technical considerations. It would be helpful, for example, to take examples of technologies that have both positive and negative human rights implications and to provide guidance on how to make necessary tradeoffs and decisions. Human rights frameworks have long had to recognise and address clashes of rights, and as a result human rights analysis has conceptual tools for making these kinds of trade-offs; human rights practitioners are therefore in a position to provide guidance on these questions.

Another important role that this inquiry can play is to engage with the question of **governance:** ie how best to address the human rights implications of technology, at all stages of technological development: (1) prospectively (ensuring consideration of human rights issues in the processes of technology development and decision-making about its deployment), (2) as a question of ongoing monitoring and response to emerging human rights concerns or breaches on technology platforms, and (3) retrospectively as a question of liability for breach, and remedy for harm. The remainder of this submission deals primarily with this set of questions. We think that there is an important role for the Commission in thinking through who should be liable for what when human rights breaches occur as a result of the use of new technologies.

We note also a further potential role for the Commission: to record, and analyse, specific gaps or problems in Australia's human rights legal framework where there are mismatches, caused by existing or imminent developments in technology, between the goals of the law and the operation of legal rules. For example, it is not clear that the way that Australian anti-discrimination law is framed and interpreted by the courts will be effective in providing a

[10] Issues here include basic concerns about access to technology: see eg Thomas et al, *Measuring Australia's Digital Divide: the Australian Digital Inclusion Index 2018*, available via http://doi.org/10.25916/5b594e4475a00 (noting that Australians with low levels of income, education, and employment are significantly less digitally included). Issues here also include the exclusionary impact of hate speech and trolling on marginalised groups in the online environment.

remedy in a case where bias has emerged as a result of the application of machine learning.[11] The Australian Privacy Foundation has identified mismatches and gaps in the privacy protection available to Australians. Criminologists have identified conflicts between child pornography laws and children's rights in the context of sexting,[12] and failures of enforcement mechanisms in relation to women's rights in the context of revenge pornography.[13] There is undoubtedly a role for the Commission in identifying important legal gaps and anomalies. However, Australia's human rights protection framework, such as it is, is constituted, not (only) of overarching principles-based legal rules, but piecemeal specific rules and exceptions embodied in numerous complex, context-specific and industry-specific pieces of legislation. A comprehensive attempt to chart the gaps may be impossible. We would therefore suggest that the Commission be very clear on the scope of the work it has undertaken, and in areas not examined, it may be better to identify areas of concern and refer for further investigation specific areas where it identifies a need for further legal investigation (for example, by the Australian Law Reform Commission).

The governance question and its relationship with human rights

As noted, a key role for the Commission is thinking through the question of governance as it relates to the development of new technologies, and how human rights fits into an overarching governance framework for technology.

There has been no shortage of discussion about technology governance. In recent times this has been particularly evident in the debate around methods for governing the technologies collectively referred to as 'artificial intelligence'.[14] Governance of these technologies has been considered in a large (and daily-growing) series of overseas government inquiries, reports, and other instruments, and giving rise to proposals for a wide range of mechanisms to assist

---

[11] See Virginia Eubanks (2017). *Automating inequality: how high-tech tools profile, police, and punish the poor* (First Edition). New York, NY: St Martin's Press. For a detailed discussion of the interaction between Australian anti-discrimination law and predictive models, see Laurence Rouesnel, 'What's the score? Preventing discrimination in an age of predictive models', unpublished thesis, copy on file with Professor Kimberlee Weatherall.

[12] See Crofts, T., Lee, M. (2013). 'Sexting', Children and Child Pornography. *Sydney Law Review*, 35(1), 85-106 (finds that child pornography laws can apply children and argues that the existing legislation lacks the capacity to discriminate properly between a broad range of activities with divergent motivations, the presence or absence of consent, and differing levels of potential harm. It concludes by suggesting that the current legislative framework has the potential to produce more harms than many of the practices it seeks to regulate).

[13] See Salter, M., Crofts, T. (2015). Responding to Revenge Porn: Challenges to Online Legal Impunity. In Lynn Comella, Shira Tarrant (Eds.), *New Views on Pornography: Sexuality, Politics, and the Law*, (pp. 233-253). California, United States: Praeger Publishers.

[14] 'Artificial intelligence' has been described as a '"A catchphrase for a cluster of technologies embedded in social systems. This includes machine learning, natural language processing, computer vision, neural networks, deep learning, big data analytics, predictive models, algorithms and robotics': Mark Latonero, *Governing Artificial Intelligence: Upholding Human Rights and Dignity,* Data and Society, https://datasociety.net/output/governing-artificial-intelligence/.

in the governance of artificial intelligence. In order to understand the role that a *human rights* perspective can play in guiding technological development, however, it is important to recognise the broader context in which the debate over governance is operating. First, we can distinguish between the range of purposes that governance mechanisms are intended to serve beyond the protection of human rights: including the promotion of public trust and public understanding of technology ('literacy'); ensuring public participation in and engagement with decisions about technology use (democratic engagement); encouraging private and/or public sector investment in or use of technologies; increasing public sector access to technological expertise; and promoting consumer rights and competition in technology and service markets. Many proposals for artificial intelligence governance are in part concerned with some combination of these other concerns. Second, governance mechanisms may target different actors: university researchers; inventors and engineers; technology developing firms; entities making decisions about whether and how to use the new technologies like machine learning or automated decision-making; public sectors and agencies. And third, governance mechanisms can seek to operate prospectively (during development phases and before implementation); during use through ongoing monitoring and adjustment in response to emerging concerns; and retrospectively to enforce rules and provide remedies for breach.

Understanding this broader context helps situate, for example, current widespread efforts to draft and promote ethical frameworks for (the development of) artificial intelligence. Such efforts are both broader, and narrower, than a concern with the protection and promotion of human rights. *Broader* in the sense that such efforts are directed to goals well beyond a concern with human rights per se. The IEEE *Ethically Aligned Design* report,[15] for example, identifies ensuring that intelligent and autonomous systems do not infringe human rights as one goal and a (first) principle in an overall report addressing a broad range of other goals and principles. Commonly identified principles directed to ethical design (and use) of artificial intelligence, in the IEEE report and others, include transparency (including explainability, comprehensibility, and traceability), accountability, beneficience (the idea that artificial intelligence or autonomous systems should act in the best interests of humans), and more. Principles of these kinds may be relevant to the protection and promotion of human rights (transparency, for example, can enable ongoing monitoring regarding the use and human rights impacts of an intelligent system), but clearly serve a range of other societal goals (including public trust in intelligent systems, public sector accountability, enforcement of competition law and consumer rights, etc).

On the other hand ethical frameworks are *narrower* in their frame than the concerns of this inquiry to protect and promote human rights. Ethical frameworks and codes of ethics are frequently directed to the technology development and design process and, in some cases,

[15] IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 'Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems, Draft Version 2' (2018) <https://standards.ieee.org/industry-connections/ec/autonomous-systems.html>.

decision-making around the deployment of technology.[16] They are not, for example, directed at key questions such as questions of liability or providing remedies for breach.[17]

We would argue, therefore, that while it may be worthwhile for the Commission to articulate points of intersection between Codes of Ethics and human rights concerns, and provide human rights-focused guidance that can inform principles promulgated as part of such systems (a point we return to below), in themselves such efforts are incomplete as an answer to the concerns raised in the issues paper. To effectively promote human rights, an enforceable human rights framework is an important starting point.

Enforceable rights

Effective protection for human rights starts with enforceable laws backed by real sanctions. The difficulties of regulating emerging technologies have, in the past, led governments to prefer self-regulatory approaches, on the basis that these are more flexible and responsive. We think that it is a mistake to turn immediately to self-regulatory and co-regulatory schemes. Effective regulation will certainly require the active participation of technology companies, but self-regulatory and co-regulatory approaches will not be sufficient on their own. Self-regulation is often a necessary component of real change, but substantial external pressure is usually required in order for real limits to develop within a company or industry group.[18] Enforceable legal obligations are a core requirement of a human rights regime that is more than aspirational.

There are gaps in Australian law where general rights with personal causes of action are urgently required in order to meet Australia's international obligations. One of the most glaring omissions from Australian law is an enforceable personal right to privacy. A personal right to privacy is long overdue, and continues to be pressing in light of new technological developments.[19] The prohibition on racial discrimination in s 18C should be defended in the

---

[16] Some recent (not yet published) research also suggests that recent statements in favour of ethical design for artificial intelligence and machine learning may be focused in particular on technical solutions to identified problems such as bias, rather than considering broader questions like the appropriate limits on the deployment of technology: see Daniel Greene, Anna Hoffman and Luke Stark, 'Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning', available at http://dmgreene.net/wp-content/uploads/2018/09/Greene-Hoffman-Stark-Better-Nicer-Clearer-Fairer-HICSS-Final-Submission.pdf.

[17] See generally Ellen Broad, *Made by Humans: The AI Condition* (Melbourne University Press, 2018).

[18] Teubner, G. (2012). Constitutional fragments: societal constitutionalism and globalization. Oxford: Oxford University Press, 84.

[19] Australian Law Reform Commission, 'Serious Invasions of Privacy in the Digital Era' (Final Report 123, June 2014).

face of ongoing attack.[20] These types of general obligations are important particularly because they are applicable across a broad and unpredictable range of future scenarios.

There are also areas of emerging risk where specific tailored legislative schemes will be required. In particular, there are serious and pressing concerns around biometrics and the widespread use of facial recognition, precision medicine, autonomous weapons, affective computing, and targeted augmented or 'mixed' reality, that may require legislative intervention in the near term.[21] Any new schemes will have to combine enforceable sanctions with sophisticated, well-resourced, and ongoing compliance monitoring. The high costs of this type of regulatory intervention means that the attention of regulators should be carefully focused on the areas posing greatest risk.[22] For these high risk areas, it is important that enforceable legal obligations are part of the regulatory response. It is likely that co-regulatory obligations will also be part of an effective strategy in these categories, but it is important that schemes designed to protect rights are also backed by real legal sanctions and effective enforcement mechanisms.[23]

It would be incomplete to refer to the need for enforceable rights without mentioning the background reality that protecting human rights in Australia continues to be challenging without an effective mechanism to allow judicial review of legislative and executive power on human rights grounds. One reason why more attention to the creation of specific, tailored *legislative* schemes are necessary in areas of high risk technology is that there is no broader legal mechanism whereby Australians can test the legality of current developments or seek remedy. Recent experience has shown that the Australian Parliament has not been able to effectively take human rights concerns into consideration when developing law that applies to new technologies. In the debate over mandatory data retention, for example, the Government was never able to convincingly address the clear human rights concerns raised by a broad network of actors.[24] Similarly, privacy rights concerns have not been adequately taken into

---

[20] For a discussion of the role that s 18C plays in protecting collective interests distinct from the kinds of individual reputational interests protected by defamation, see Rolph, D. (2015). Racial discrimination laws as a means of protecting collective reputation and identity. In Matthew Rimmer (Eds.), *Indigenous Intellectual Property: A Handbook of Contemporary Research*, (pp. 477-494). Cheltenham: Edward Elgar Publishing.

[21] See, for example, IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 'Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems, Draft Version 2' (2018) <https://standards.ieee.org/industry-connections/ec/autonomous-systems.html>

[22] Michael Guihot, Anne F Matthew and Nicolas P Suzor, 'Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence' (2017) 20(2) *Vanderbilt Journal of Entertainment and Technology Law* 385 <https://eprints.qut.edu.au/109926/>.

[23] See Ian Ayres and John Braithwaite, *Responsive Regulation* (Oxford University Press, 1994) 4, noting that responsive regulation still requires government to assert a 'willingness to regulate more intrusively'.

[24] Nicolas P Suzor, Kylie M Pappalardo and Natalie McIntosh, 'The Passage of Australia's Data Retention Regime: National Security, Human Rights, and Media Scrutiny' (2017) 6(1) *Internet Policy Review* <https://policyreview.info/articles/analysis/passage-australias-data-retention-regime-national-security-human-rights-and-media>.

account in a range of other surveillance projects by the Australian Government.[25] These types of issues are frequently posited as a trade-off between security and basic rights to privacy; this is a false binary that works to delegitimise privacy interests and often leads to legislation that is poorly tailored to achieving its goals.[26]

In other jurisdictions, courts have played a crucial role in limiting legislative and administrative attempts to use technology in a way that impermissibly infringes on fundamental rights. For example, the French Constitutional Council struck down the first iteration of a regime that would have terminated the internet access of people alleged to have infringed copyright.[27] The Court of Justice of the European Union held that an indiscriminate data retention obligation went beyond what was necessary and proportionate to achieve its objectives to fight 'serious crimes' and was therefore incompatible with the fundamental right to privacy and to data protection.[28] The European Court of Human Rights recently found that aspects of the UK surveillance regime violated fundamental rights to privacy and expression.[29] A strong Bill of Rights can also usefully enable the judiciary to adapt the law in the face of technological change when private actors are infringing on rights. For example, the Court of Justice of the European Union was able to use the rights embedded in the Charter of Fundamental Rights of the European Union to impose new obligations on search engines to remove personal information in certain circumstances.[30]

Effective oversight by the judiciary is extremely important to ensuring that public regulatory schemes that impact on human rights are necessary and proportionate. Although the debate about the introduction a Bill of Rights in Australia has been drawn out, there is momentum towards real change in several Australian jurisdictions. Ideally, Australia should introduce a constitutionally-entrenched Bill of Rights. Constitutional change is very difficult, particularly where it would limit the powers of Government, but we think it is important to continue this

---

[25] Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40(1) *University of New South Wales Law Journal* 121 <http://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2017/09/40-1-11.pdf>.

[26] Monique Mann et al, 'The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)Balance in Australia' [2018] *International Communication Gazette* <https://eprints.qut.edu.au/112150/>; Monique Mann, 'Privacy in Australia: Brief to UN Special Rapporteur on Right to Privacy' (Report, Australian Privacy Foundation, 15 August 2018) <https://privacy.org.au/2018/08/15/australian-privacy-foundation-provides-background-brief-on-all-the-privacy-omnishambles-to-un-special-rapporteur-on-privacy/>.

[27] *Loi favorisant la diffusion et la protection de la création sur internet* (2009) Décision n° 2009-580 DC (Unreported, Conseil Constitutionnel, France, 10 June 2009); See further Nicolas Suzor and Brian Fitzgerald, 'The Legitimacy of Graduated Response Schemes in Copyright Law' (2011) 34 *UNSWLJ* 1 <https://eprints.qut.edu.au/43926/>.

[28] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* [2014] Grand Chamber, European Court of Justice C-293/12 and C-594/12 (8 April 2014).

[29] *Big Brother Watch and Others v. the United Kingdom*, European Court of Human Rights 58170/13, 62322/14, 24960/15 (13 September 2018).

[30] *Google Spain SL v Gonzalez* [2014] Court of Justice of the European Union C-131/12 (13 May 2014).

discussion. In the meantime, a Commonwealth Human Rights Act that provides real remedies should still be the first goal of meaningful legal protection for rights in Australia.

Liability and responsibility in human rights by design: who should be liable?

A number of recent reports that consider the governance of technology, including in particular the development of artificial intelligence, have raised the urgent need for a greater clarity around responsibility, culpability, liability and accountability during development and deployment.[31]

In developing an effective multi-layered model of regulation to promote human rights in the face of rapid technological change, it is important to note some general principles that should guide the imposition of obligations on designers, manufacturers, and operators of technical tools. Liability under our legal system generally focuses on wrongdoing, and there is a basic principle that liability should generally focus on harm that has occurred as a result of direct conduct or a dereliction of a clear duty. It is generally uncontroversial to say that it is appropriate to impose liability on people who use technological tools in ways that harm human rights. It is more difficult to draw the boundaries of liability as it applies to those who design or deploy a technical system that is then used by a third party to cause harm. General principles of causation and responsibility suggest that, ordinarily, those who develop or deploy tools that are harmful may legitimately be held accountable where those tools are (a) are designed to cause harm; (b) designed in a way that harm is likely to be an ordinary consequence; (c) cause harm when used by a person under real control or supervision of the designer or operator.[32] These situations are conventionally where we could say that technology developers have a clear responsibility that could be backed by legal liability when their tools are used to cause harm.

In circumstances where general purpose tools can be used in harmful and non-harmful ways, it may not be appropriate to impose secondary liability for harm on the developer. Imposing liability in these circumstances will often lead to great uncertainty, because the acts giving rise to liability will often be too far removed from the wrongful act. Technology companies are often shielded from legal liability from the acts of their users over whom they lack control. Generally speaking, limiting liability for the acts of users that are beyond a developer's control is important to ensure that the law is able to focus on wrongdoing in a way that can guide behavior.[33] Indeed, the lack of strong protection for technology companies from liability for the

---

[31] See for example IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 'Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems, Draft Version 2' (2018) <https://standards.ieee.org/industry-connections/ec/autonomous-systems.html>.

[32] See Kylie Pappalardo, *A Tort Law Framework for Copyright Authorisation* (PhD Thesis, Australian Catholic University, 2016) <https://eprints.qut.edu.au/102226/> (applying general tortious principles of causation and responsibility to intermediary liability in copyright law).

[33] Kylie Pappalardo, *A Tort Law Framework for Copyright Authorisation* (PhD Thesis, Australian Catholic University, 2016) <https://eprints.qut.edu.au/102226/>.

acts of their users can lead to negative impacts on human rights as companies move to mitigate their liability risks by clamping down on user freedoms.[34]

Human rights and design

Nevertheless, mitigating the impact of new technologies on human rights will require careful attention to human rights as part of the design process. The *UN Guiding Principles on Business and Human Rights* provide some guidance about the responsibilities of developers of new technologies. The Guiding Principles have a number of discrete implications for technology companies: first, that companies should exercise due diligence to identify their impact on human rights; second, that due diligence requires them to take steps to prevent and mitigate negative impact through their policies, procedures, and design choices; and third, that firms have some responsibility to develop effective remedies where human rights have been violated.

This language of responsibility under human rights law is much different to established concepts of legal liability. However, binding legal obligations can be usefully added to this framework. While secondary liability should not usually accrue for harmful uses of technology beyond the developer or manufacturer's control, it will often be useful to create new obligations that set enforceable standards for design. The distinction is subtle, but important. For law to adequately guide the development of technology, the obligations of designers must be clearly explained. Rather than use the relatively blunt instrument of liability, it is often preferable to set clear legal obligations, backed by real sanctions, that require developers to take certain steps to consider the impact of their tools on human rights and to implement safeguards to limit or mitigate potential harms. This would mean, for example, setting expectations that developers follow best practices in designing new tools to limit the extent to which personal information is captured and stored, or to ensure that tools are accessible to people with disabilities. There is also a potential role for the Commission and for government to play in fostering industry dialogue to develop best practice guidelines and industry codes of conduct in relation to the promotion of human rights.

Industry guidance and governance frameworks

Our primary position is that enforceable legal rights are necessary to an effective human rights protection framework, and that a key role the Commission can play is in developing thinking around questions of liability.

We recognise however that effective protection of human rights also requires recognition of human rights problems to be part of the whole process of technology development and deployment. Therefore another key opportunity is for the Commission to directly influence the development and deployment of technologies that are likely to have an impact on human rights *prospectively,* by helping provide more effective guidance to industry and public agencies. The IEEE *Ethically Aligned Design* report, arising from an inclusive and extensive consultation

---

[34] See, for example, 'Manila Principles on Intermediary Liability: Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation' <https://www.manilaprinciples.org/> (arguing that internet intermediaries should not be held responsible for the actions of their users).

process, includes two key draft recommendations for society to assure the safety and security of autonomous and intelligent systems (A/IS):

1. "Governance frameworks, including standards and regulatory bodies, should be established to oversee processes assuring that the use of A/IS does not infringe upon human rights, freedoms, dignity, and privacy, and of traceability to contribute to the building of public trust in A/IS".
2. "A way to translate existing and forthcoming legal obligations into informed policy and technical considerations is needed. Such a method should allow for differing cultural norms as well as legal and regulatory frameworks."[35]

These recommendations mirror the expectation of the United Nations *Guiding Principles on Business and Human Rights* that States will provide effective guidance to business enterprises on how to respect human rights throughout their operations.[36]

We suggest that the Commission could play an important role in fostering the development of clear and considered guidelines addressing the question of *human rights protection* in the development, implementation, application and review of automated decision making and other key technologies: whether those guidelines are part of broader instruments addressing other goals or stand-alone guidelines. While there are other guidance documents that exist, there is little clear guidance that is specific to the Australian legal or social context. This is important because, as the IEEE Report notes, the development and deployment of such systems needs to take into account both differing cultural norms as well as differing legal and regulatory frameworks. In thinking about the impact of such technologies on freedom of expression, for example, it would be a mistake to assume that guidelines developed in the United States can simply be transplanted to Australia.

Importantly, guidelines and governance frameworks are required for both public and private sectors. Updated risk management frameworks are urgently needed for the public sector in Australia. We note, for example, the many concerns raised around automated debt recovery by the Australian government, and the fact that the Australian government's *Better Practice Guide on Automated Assistance in Administrative Decision Making* has not been updated since 2007. Renewed guidelines in light of the findings of this Inquiry should particularly deal with concerns about the limited choice presented to individuals in the public deployment of new technologies, as well as concerns around the collection and reuse of highly sensitive data by government (including financial, health, and census data).

We also suggest that the Commission could provide guidance that helps businesses and public agencies work through appropriate responses when they identify that they have participated in adverse human rights impacts. This type of guidance could be particularly helpful for technology developers and for firms and public agencies who implement tools developed by others.

---

[35] IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 'Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems, Draft Version 2' (2018) <https://standards.ieee.org/industry-connections/ec/autonomous-systems.html>.

[36] John Ruggie, 'Business and Human Rights: Towards Operationalizing the "Protect, Respect and Remedy" Framework' (A/HRC/11/13, UN Human Rights Council, 22 April 2009).

Effective co-regulation

Regulating the development and deployment of advanced technologies is a notoriously difficult task. One of the fundamental challenges of regulating technology is that the technological development often outstrips the pace of innovation in regulatory tools that might be used to govern it.[37] In these situations, regulation lags behind or in some circumstances 'decouples' from the technology it seeks to address.[38] The difficulty is exacerbated because public regulatory agencies face major challenges in monitoring and understanding the social impacts of technological change. Private companies are investing heavily in research and development, and there are information asymmetries between those companies and public regulators seeking to understand the potential impact of new technologies.[39] The design of many of the new technologies considered in the Issues Paper is often opaque, largely incomprehensible,[40] and sometimes even unknowable.[41] Even if regulators are able to obtain better information from developers, they are often not well equipped or resourced to understand new tools in a way that allows them to predict what impacts they may have on individuals, societies and economies.[42]

The challenge of regulating the development and deployment of technology is a challenge of regulating a complex system with many separate interacting components. An effective regulatory response has to pay attention to how regulation can operate in 'decentred' or 'polycentric' environments.[43] The imposition of 'top-down', 'command-and-control' obligations are often not effective or not sufficient in these environments. Effective 'decentred' regulation

---

[37] See Gary E Marchant, Braden R Allenby and Joseph R Herkert (eds), The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem (Springer, 2011).

[38] Braden R Allenby, 'The Dynamics of Emerging Technology Systems' in Kenneth W Abbott, Gary E Marchant and Braden R Allenby (eds), *Innovative Governance Models for Emerging Technologies* (Edward Elgar Publishing, 2013) 43.

[39] Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (Oxford Scholarship Online, 2008) <http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199276806.001.0001/acprof-9780199276806>; Graeme Laurie, Shawn HE Harmon and Fabiana Arzuaga, 'Foresighting Futures: Law, New Technologies, and the Challenges of Regulating for Uncertainty' (2012) 4(1) *Law, Innovation and Technology* 1.

[40] Perri 6, 'Ethics, Regulation and the New Artificial Intelligence, Part II: Autonomy and Liability' (2001) 4 *Inf. Commun. Soc* 406, 410.

[41] Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard Univ. Press, 2015).

[42] MC Stephenson, 'Information Acquisition and Institutional Design' (2011) 124(6) *Harvard Law Review* 1422; H Bakhshi, A Freedman and PJ Heblich, 'State of Uncertainty: Innovation Policy through Experimentation' (NESTA, 2011); Gregory N Mandel, 'Regulating Emerging Technologies' (2009) 1(1) *Law, Innovation and Technology* 75.

[43] Julia Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (2008) 2(2) *Regulation & Governance* 137.

must be 'hybrid (combining governmental and non-governmental actors), multi-faceted (using a number of different strategies simultaneously or sequentially), and indirect'.[44]

There is no easy answer to the difficult challenges of regulating emerging technologies. Given the complexity of the issues involved, however, we believe that it is important to incubate a strong set of institutions that are able to hold those who develop and deploy risky technological tools to account. Developing a good understanding of the impact of new technologies requires a great deal of work to understand their operation at a systems level. Because information is so fragmented, this can only be done through extensive collaboration. There is a pressing need for strong, multistakeholder networks of industry, civil society, academic researchers, journalists, and public agencies that are empowered to monitor the development and deployment of new technologies against human rights standards.[45] We highlight particularly the need for not only greater transparency from technology companies, but simultaneously for real commitments to funding critical research and ongoing opportunities for multistakeholder collaboration and sharing of information and expertise.

Privacy

The Commission correctly identifies privacy as a key right affected by developing digital technology. Privacy is affected by the expanding *collection* - by both government and the private sector - of information that relates to human beings, their identity, activities, private life and physical and biometric features; and the expanding potential for *linkage* and ongoing *reuse* of such data including reliance on data in decision-making, both automated, and human decision-making informed by data analysis. These changes impact privacy, understood as a rich, contextually-dependent, multi-dimensional right promoting an individual's ability to object to and control collection and use of personal information; to enjoy some seclusion from intrusion into the private sphere by the state and private actors, and to exercise control and agency over their social situation and choices without interference. New technologies - especially the large-scale collection and analysis of data and ability to use that analysis to target individuals and change their information environment in ever-more-fine-grained ways, highlight the critical connection between privacy and human autonomy and agency.

A voluminous research literature sets out in detail how inadequate Australian legal and institutional frameworks are for protecting Australians' rights to privacy. There is no

---

[44] Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (2001) 54(1) *Current Legal Problems* 103, 111.

[45] See, e.g. Nicolas Suzor, Tess Van Geelen and Sarah Myers West, 'Evaluating the Legitimacy of Platform Governance: A Review of Research and a Shared Research Agenda' (2018) 80(4) *International Communication Gazette* 385 <https://doi.org/10.1177/1748048518757142> (discussing the need for a broad range of institutions to help understand complex systems of internet governance).

constitutional right to privacy[46] and no cause of action for serious invasion of privacy.[47] In relation to the collection and use of personal data by the *private* sector, the *Privacy Act 1988* (Cth) provides little protection.[48] It has significant exemptions (eg for firms with turnover less than AU$3M), and is structured around a 'notice and consent' model that enables significant collection and use as long as such use is set out in a document like a privacy policy; research demonstrates that it would be entirely infeasible for most people to read, let alone understand or negotiate around these policies, even where such negotiation possible.[49] The *Australian Privacy Principles* are enforceable only by the Office of the Australian Information Commissioner which is underfunded and lacks independence. In relation to collection and use of personal data by government, the literature amply sets out the vulnerability of Australians to mass surveillance, collection of and linking of data.[50] These deficiencies in Australian privacy law can be seen in sharp contrast to the situation in the European Union and United Kingdom: the Snowden revelations from 2013 of mass surveillance and data gathering by the Five Eyes partnership (US, UK, Australia, Canada and New Zealand) spurred a series of legal challenges to aspects of this surveillance programme and the privacy frameworks offered to EU citizens' data by Five Eyes countries. While Australia is a member of this alliance, similar challenges to Australia's surveillance activities and deficiencies in privacy protection are not possible due to the lack of constitutional protection for privacy. This can be clearly seen regarding data retention measures, which were invalidated in the EU for their interference with the rights to privacy and data protection in the *Digital Rights Ireland* case, but shortly afterwards Australia adopted similar legislation which remains in force to this day.

In addition to recognising the gaping holes in Australia's legal framework, this Commission should address problematic tendencies in the Australian policy debate around privacy, and the development and use of data sharing, data analytics and data-driven decision-making. First, there is a tendency in Australian policy debates to promulgate a myth that Australians'

---

[46] See Williams, G and Reynolds, D (2017) *A charter of rights for Australia*, Sydney, NSW: NewSouth Publishing. Some individual states have legislated human rights instruments but they are not enforceable.

[47] Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era: Final Report (2014).

[48] See eg Greenleaf G (2001) ' 'Tabula rasa': Ten reasons why Australian privacy law does not exist' (2001) 24 *UNSWLJ* 262.

[49] See eg McDonald, A and Cranor, L, 'The Cost of Reading Privacy Policies' (2014) 4 *I/S: Journal of Law and Policy for the Information Society* 543-568. Sensitive data (health, genetic, biometric, criminal record etc) receives some additional protection: *Australian Privacy Principles* Principle 3.3.

[50] Bronnitt S and Stellios J, 'Regulating telecommunications interception and access in the twenty-first century: Technological evolution or legal revolution? (2006) 24(4) *Prometheus* 413-428; De Zwart M, Humphreys S and van Dissel B (2014) 'Surveillance, big data and democracy: Lessons for Australia from the US and UK' (2014) 37(2) *UNSWLJ* 713-747; Lachmayer K and Witzleb N, 'The challenge to privacy from ever increasing state surveillance: A comparative perspective' (2014) 37 *UNSWLJ* 748-783; Mann, M, Daly, A, Wilson, M and Suzor, N, 'The limits of (digital) constitutionalism: Exploring the privacy-security (im)balance in Australia' (2018) *International Communication Gazette* https://doi.org/10.1177/1748048518757141; Mann, M and Smith, M, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40 *UNSWLJ* 121-145 http://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2017/09/40-1-11.pdf.

use of social media platforms such as Facebook, Instagram and others is evidence that they neither understand, or care about, privacy. Those who promulgate this myth fail to recognise the significant social costs, for at least some proportion of Australians, of not engaging with social media, and fails to recognise too the steps Australians do take to manage their own accessibility via such platforms.

Evidence suggests that concerns about privacy grow alongside social media use over time. A significant body of research demonstrates that Australians care about their privacy, and actively take steps to protect their privacy.[51] There is also evidence that people take more care than is commonly imagined in negotiating their privacy; people may be prepared to trade some privacy for convenience in some circumstances, but often maintain limits that reflect their preferences.[52] Worryingly, for many, taking steps to protect their privacy does not lead to feelings of control or agency. A recent study found that 67% of Australians take active steps to protect their privacy, but only 38% felt that they can control their privacy online.[53] This research also shows that certain populations showed more concern about privacy. Young people, people from English speaking backgrounds, and those who have had their privacy violated, are all significantly less confident in their own capacity to protect their privacy online. Importantly, frequent social media commenting and posting is significantly related to both concern and confidence about the capacity to protect individual digital privacy. This suggests that simply withdrawing from interactions and actively posting on social media platforms will not make individuals feel that they are more protected or that their data is safer online. The major point here is that policy responses should not prefer abstinence from social media and other online services as a solution to privacy, but instead prioritise measures that can meaningfully improve the autonomy of people to make choices and exercise control over their privacy.

Second, Australian policy discussions in recent times have asserted the importance of *social licence* and public *trust* without addressing seriously how either is to be secured.[54] Both (1) an effective legal and regulatory framework that provides for accountability for interferences with privacy and genuine and accessible redress, and (2) serious government and policymaker engagement with community understandings and expectations of human rights including are important elements of building public trust.[55] Importantly, Australians are concerned about invasions of privacy from both corporations and the public sector. In a representative survey, the Digital Rights in Australia Report found that 57% of Australians were concerned about their

---

[51] See for example the data produced in Goggin, G; Vromen, A, Weatherall, K, Martin, F, Webb, A, Sunman, L, Francesco, B, *Digital Rights in Australia* (2017), available at https://ses.library.usyd.edu.au/handle/2123/17587.

[52] Goggin, G; Vromen, A, Weatherall, K, Martin, F, Webb, A, Sunman, L, Francesco, B, *Digital Rights in Australia* (2017), available at https://ses.library.usyd.edu.au/handle/2123/17587, 19.

[53] Goggin, G; Vromen, A, Weatherall, K, Martin, F, Webb, A, Sunman, L, Francesco, B, *Digital Rights in Australia* (2017), available at https://ses.library.usyd.edu.au/handle/2123/17587, 16.

[54]See, e.g., Productivity Commission, *Data availability and use* (2017), available at https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf, 177-9.

[55] This was a key purpose of the *Digital Rights in Australia* research project at the University of Sydney: see Goggin, G; Vromen, A, Weatherall, K, Martin, F, Webb, A, Sunman, L, Francesco, B, *Digital Rights in Australia* (2017), available at https://ses.library.usyd.edu.au/handle/2123/17587.

privacy being violated by corporations, and 47% were concerned about government violating their privacy.[56] A large majority (78%) want to know what social media companies do with their personal data.[57]

Third, debates construct the information environment as one of threat to national security: justifying the de-prioritising of privacy in order to promote the expansion of law enforcement powers.[58] This is understandable: there is evidence of increased support for surveillance measures which are described as being implemented for the purpose of prevention of terrorism.[59] Governments have also been able to secure bi-partisan support for controversial legislative measures like data retention on national security grounds, even without fully articulating the benefits or addressing substantial human rights concerns.[60] In reality, however, measures that are described as necessary for counter-terrorism efforts or law enforcement may give rise to uses of data in a much wider range of circumstances than is consistent with expectations that might be held by the Australian public:[61] a fact that is corrosive of rights, democracy and public trust in expanded data-sharing and use.

Finally, current debates around data-sharing and data use in analysis and decision-making risk too often use outdated conceptions of privacy and inadequate risk analysis frameworks. The prioritisation of notice and consent, in particular, is likely to prove manifestly inadequate in light of rapidly developing capacity for data linkage, data use, individualised targeting of the information environment, and automated decision-making. Similarly, policies that focus on improving data literacy among consumers are not adequate for addressing real privacy risks in contexts where there are constraints the ability of people to consent -- including, but not limited to, information overload, external pressure to consent, or manipulation of the information environment through targeted profiling. The challenges posed by contemporary technologies that make extensive secondary uses of data and enable the linkage of multiple data sets over an extended period of time are not adequately addressed either by consent at

---

[56] Goggin, G; Vromen, A, Weatherall, K, Martin, F, Webb, A, Sunman, L, Francesco, B, *Digital Rights in Australia* (2017), available at https://ses.library.usyd.edu.au/handle/2123/17587, 16, 22.

[57] Goggin, G; Vromen, A, Weatherall, K, Martin, F, Webb, A, Sunman, L, Francesco, B, *Digital Rights in Australia* (2017), available at https://ses.library.usyd.edu.au/handle/2123/17587, 18.

[58] Mann, M, Daly, A, Wilson, M and Suzor, N, 'The limits of (digital) constitutionalism: Exploring the privacy-security (im)balance in Australia' (2018) *International Communication Gazette*

[59] Goggin, G; Vromen, A, Weatherall, K, Martin, F, Webb, A, Sunman, L, Francesco, B, *Digital Rights in Australia* (2017), available at https://ses.library.usyd.edu.au/handle/2123/17587, p 24-5.

[60] Nicolas P Suzor, Kylie M Pappalardo and Natalie McIntosh, 'The Passage of Australia's Data Retention Regime: National Security, Human Rights, and Media Scrutiny' (2017) 6(1) *Internet Policy Review* <https://policyreview.info/articles/analysis/passage-australias-data-retention-regime-national-security-human-rights-and-media>.

[61] Limited evidence gathered in the context of the *Digital Rights in Australia* research via an online focus group suggest that in the context of a more nuanced discussion around hypotheticals, different views can emerge around the use of data for a range of different forms of government use: in the context of the online focus group discussion, some relatively low-level public health use of data was described by some participants as 'Big Brotherish' or 'creepy' (p 26). This research is, however, limited and there is an urgent need for further exploration of community expectations of rights in the context of data gathering, data linkage, data use and decision-making.

the time of collection or by risk management frameworks like the 'Five Safes' model used by some government agencies that focus on relatively static stores of personal information.[62] There is an urgent need to revise risk management guidance in light of recent technological advances. The Australian Government's own framework for guiding the use of automated technology in public decisionmaking, for example, is, as noted above, now more than a decade old.[63]

Structural inequality

Some of the most pressing challenges are underlying structural inequalities that are amplified and exacerbated by technology. Australia still faces important challenges in overcoming the 'digital divide'; a 2017 report found that 'Australians with low levels of income, education, and employment are significantly less digitally included.'[64] Levels of access to digital technology and services are particularly concerning for people aged over 65, for people on low incomes, for people with a disability, and for people in rural and remote areas. Affordability of internet services is becoming more of a problem, particularly for people on low incomes. Worryingly, the divide has widened in recent years for low income and older Australians. Digital inclusion and access to important communications and assistive technologies is a core challenge that must be addressed as a priority when thinking about the intersection of human rights and technology. Remote indigenous communities also face important issues regarding safety and access to digital technologies that need particular attention.[65]

Digital technologies can amplify and reinforce existing structural inequalities in ways that are often opaque. Many of the issues canvassed in the Issues Paper point to the need for increased attention to human rights implications as part of the design process of new technologies. The UN Guiding Principles on Business and Human Rights articulate the proposition that technology companies have a responsibility to address harms that they enable or facilitate. The responsibility of technology firms under the Guiding Principles extend significantly beyond legal liability. The Guiding Principles particularly provide insight into the responsibility of technology companies to address broader social inequalities that are often reproduced and can be exacerbated by their systems. Ultimately, technology companies can avoid infringing on the human rights of others by considering human rights throughout the design and operation of their systems. One of the most dangerous engineering practices in

---

[62] See Australian Bureau of Statistics, 'Managing The Risk Of Disclosure: The Five Safes Framework' (2017) http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features4Aug%202017?opendocument&tabname=S#FIVESAFES

[63] Australian Government, 'Automated Assistance in Administrative Decision-Making: Better Practice Guide' (2007) https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf

[64] Julian Thomas et al, 'Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2017' (1 August 2017) <http://apo.org.au/node/97751>, 5.

[65] Rennie, E. Yunkaporta, T. Holcombe-James, I. (2018). *Cyber safety in remote Aboriginal communities: final report*. Melbourne: Digital Ethnography Research Centre, available at <http://apo.org.au/node/172076>.

this regard is to treat the technology being developed as neutral and, as a consequence, to avoid making considered choices about how potential harmful uses of the tools can be mitigated.

There are many examples of apparently 'neutral' technical tools that are used in ways that reflect and reinforce structural inequalities. Ordinary, everyday telecommunications systems and apps are routinely used by perpetrators of domestic violence to extend their ability to coerce and control their current or former partners.[66] The pervasive abuse and harassment of women and minority groups on social media has a strong cumulative negative effect and drives marginalised people offline.[67] Search engines learn biases in existing data and help perpetuate ongoing discrimination.[68] Predictive models and automated decisionmaking operate to entrench existing patterns of discrimination.[69] Advertising systems are used to discriminate on protected characteristics.[70] The search algorithms and rating systems of peer economy platforms are routinely used in ways that discriminate against marginalised groups.[71] Other examples are plentiful in the mainstream media and academic literature.

In many cases, these discriminatory results are not the result of intentional bias, but rather of the lack of attention to how a tool is used in a discriminatory way. These are manifestations of underlying systemic inequality that are amplified and reinforced by technical tools. In order to address discrimination at a network or systems level, it will be necessary for technology businesses to continuously monitor these impacts, and to work to design their tools to limit the potential for harm.[72] The UN Guiding Principles set out the general responsibilities of businesses, but there is a need for greater guidance about what, exactly, technology

---

[66] Molly Dragiewicz et al, 'Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms' [2018] *Feminist Media Studies* 1.

[67] Nicolas P Suzor et al, 'Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online' [2018] *Policy & Internet* <https://eprints.qut.edu.au/121223/>; Stefanie Duguay, Jean Burgess and Nicolas Suzor, 'Queer Women's Experiences of Patchwork Platform Governance on Tinder, Instagram, and Vine' [2018] *Convergence* https://doi.org/10.1177/1354856518781530.

[68] Safiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism (New York University Press, 2018).

[69] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (StMartin's Press, First Edition., 2017).

[70] Julia Angwin, Ariana Tobin and Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude…* (21 November 2017) ProPublica <https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin>.

[71] Nicolas P Suzor, Tess Van Geelen and Katherina Drinkuth, 'Submission to the Opportunities for Personalised Transport Green Paper' (Report, 2016) <https://eprints.qut.edu.au/96262/>; Alice Witt, Nicolas Suzor and Patrik Wikström, 'Regulating Ride-Sharing in the Peer Economy' (2015) 1(2) *Communication Research and Practice*.

[72] Nicolas P Suzor et al, 'Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online' [2018] *Policy & Internet* <https://eprints.qut.edu.au/121223/>.

companies should do, and better monitoring and reporting from third parties to drive increase uptake.

These issues also raise the need for new forms of regulation for anti-discrimination law that can impose obligations at the systems level for systems that have the effect of enabling discrimination. It is not necessarily desirable to hold technology companies liable for discriminatory acts of their users; such an obligation would likely introduce legal risk that would be largely unmanageable. However, the businesses that profit from connecting individuals do bear some responsibility to address violations of human rights that are carried out through their networks. Apart from the non-binding obligations under the UN Guiding Principles, we suggest that new obligations should be crafted to require technology companies to monitor, respond to, and report on discrimination on their networks. it is imperative that technology companies be called to account for how they identify and respond to systemic bias on prohibited characteristics.