

Australian Human Rights Commission Human Rights and Technology Issues Paper

October 2018

Australian Human Rights Commission
Level 3, 175 Pitt Street
Sydney NSW 2000

By email: tech@humanrights.gov.au

Contact: **David Turner**
President, NSW Young Lawyers

Eva Lu
NSW Young Lawyers Communications, Entertainment and Technology Committee

Editor: Eva Lu

Contributors: Lee Elsdon, Ravi Nayar, Onur Saygin and Sophia Urlich

The NSW Young Lawyers Communications, Entertainment and Technology Law Committee (Committee) makes the following submission in response to the Australian Human Rights Commission's Human Rights and Technology Issues Paper.

NSW Young Lawyers is a division of The Law Society of New South Wales. NSW Young Lawyers supports practitioners in their professional and career development in numerous ways, including by encouraging active participation in its 15 separate committees, each dedicated to particular areas of practice. Membership is automatic for all NSW lawyers (solicitors and barristers) under 36 years and/or in their first five years of practice, as well as law students. NSW Young Lawyers currently has over 15,000 members.

The Communications, Entertainment and Technology Law Committee (**Committee**) of NSW Young Lawyers aims to serve the interests of lawyers, law students and other members of the community concerned with areas of law relating to information and communication technology (including technology affecting legal practice), intellectual property, advertising and consumer protection, confidential information and privacy, entertainment, and the media. As innovation inevitably challenges custom, the CET Committee promotes forward thinking, particularly about the shape of the law and the legal profession.

1. Introduction

The Communications, Entertainment and Technology Law Committee (**Committee**) of NSW Young Lawyers welcomes the opportunity to comment on the Human Rights and Technology Issues Paper.

The Committee supports the Australian Human Rights Commission's project to explore what the rise of modern technology means for our human rights.

The Committee recognises the unprecedented potential and opportunity that modern technology brings. The Committee also recognises that modern technology, when misused or used without the necessary checks and balances, could divide and exclude, rather than act as a force for inclusion and equality.

This submission proposes potential legislative and non-legislative solutions to protect and promote human rights in the proliferation of modern technology.

The Committee considers it critical that every attempt should be made to alleviate any negative impact or disadvantage created by the implementation of new technology. Where this is impossible or unfeasible, strategies should be developed to assist vulnerable or disadvantaged groups to adapt to new technology.

2. Key Issues for Particular Groups within the Australian Community

Access

Australia is currently experiencing two simultaneous trends, an ageing population and rapid technology diffusion.¹ Older people are typically slower to adopt new technology and are more apprehensive about doing so.² A 2013 US study³ found that older people were "willing to adopt new technologies when their usefulness and usability surpassed feelings of inadequacy".⁴ Despite their slow adoption, new technology promises to

¹ Meg Morris et al, 'Smart Technologies for Older People: a Systematic Literature Review of Smart Technologies that Promote Health and Wellbeing of Older People Living at Home' (Report, University of Melbourne, 2012) 7 <https://networkedsociety.unimelb.edu.au/__data/assets/pdf_file/0008/1661327/Smart-technologies-for-older-people.pdf>.

² Eleftheria Vaportzis, Maria Giatsi Clausen and Alan J Gow, 'Older Adults Perceptions of Technology and Barriers to Interacting with Tablet Computers: A Focus Group Study' (2017) 8 *Frontiers in Psychology* 1687 <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5649151/>>.

³ Melinda Heinz et al, 'Perceptions of Technology among Older Adults' (2013) 39(1) *Journal of Gerontological Nursing* 42.

⁴ Vaportzis, Clausen and Gow, above n 2.

improve the lives of older people and prolong our life expectancy, with apps and devices allowing easier access to services, virtual medical services and tools to assist with independence.

On the other end of the generation spectrum, the early adopters of new technology, children and young people, have experienced substantial enhancements in their access to information and education with the use of new educational tools. New technologies have also promoted self-reliance and facilitated active participation of disabled children in the classroom. However, new technologies also give children and young people the opportunity to encounter "unparalleled amounts of both filtered and unfiltered information and imagery, which they need to navigate and manage", often without the guidance or support of adults.⁵ However, if new technologies do not accommodate the diversity of cultures and languages, it could significantly hamper the development of digital skills, literacy and access to quality education in children from culturally and linguistically diverse backgrounds.

Irrespective of whether one is an early or late adopter of new technology, access to technology itself can prove to be a key issue for particular groups of the community. While there is no express human right to Internet access, the United Nations passed a resolution emphasising the importance of Internet access for the fulfillment of many human rights and called for states to take measures to work towards universal access to the Internet.⁶ However, due to various reasons such as location, availability and cost, a large number of people, including Aboriginal and Torres Strait Islander peoples, older people, people from lower-socioeconomic backgrounds and people from remote communities, have limited access to electricity, devices, phone and data connection, and the Internet. Such people are deprived of the benefits of new technology and have fallen on the wrong side of the 'digital divide', for example the 2018 Australian Digital Inclusion Index show that people in the lowest household income quintile have a digital inclusion score of 41.3, which is 30.8 points lower than those in highest household income quintile.⁷ If more could be done to make these services universally available, at reasonable cost, quality of life and equality may be significantly improved. For example, a strong data connection would enable online health services to assist people who have limited access to local on-the-ground medical services.

⁵ Megan Mitchell, 'Children's Rights in a Changing World' (Speech delivered at the Association of Children's Welfare Agencies Conference 2014, Sydney, 20 August 2014) <<https://www.humanrights.gov.au/news/speeches/childrens-rights-changing-world>>.

⁶ *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, GA Res 32/20, 32nd sess, Agenda Items 3, UN Doc A/HRC/32/L.20 (27 June 2016) <https://www.article19.org/data/files/Internet_Statement_Adopted.pdf>.

⁷ Julian Thomas et al, 'Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2018' (Report, RMIT University, 2018) 5 <<https://digitalinclusionindex.org.au/wp-content/uploads/2018/08/Australian-digital-inclusion-index-2018.pdf>>.

Cyberbullying and Privacy

Anonymity online and wide use of the Internet means it is now more often used as a platform to defame, harass and abuse people, despite piecemeal cyberbullying legislative attempts such as *the Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* (Cth) to address such behaviour. Bullying taps into societal undertones of prejudice and discrimination and often impacts people with protected characteristics of race, religion, children and young people, sexuality, gender and disability.⁸ It can occur anonymously, at any time, in any place, allows for a potentially infinite audience to view or participate and may have a permanency of expression, as information posted online can be difficult or in some cases, impossible for remove.⁹ A Ditch the Label and Brandwatch analysis of 19 million tweets over a four-year period found that there were almost 5 million cases of misogyny, 7.7 million cases of racism, and 390,296 instances of homophobia on Twitter alone.¹⁰

Cyberbullying not only undermines the objective of the Internet to promote a freedom of expression, but instead has created an environment where expression, often by those protected groups, is suppressed. An Amnesty International online poll found that of the women polled who experienced online abuse or harassment, 76% made some changes to the way they used social media platforms such as increasing their privacy and security setting and 32% made changes to the way they expressed themselves online in response to abuse or harassment.¹¹ In more extreme forms of cyberbullying, forms of abuse or harassment extend beyond the Internet with 29% of the women polled reporting their physical security and privacy was also compromised through the unauthorised sharing of their personal information, such as their address and phone number.

Further, new technology often fails to take into account the necessary differences between adults and children and young people, particularly in terms of their competencies, capacities and special vulnerability arising from developmental differences, meaning children and young people may be exposed to inappropriate and harmful content. In a 2016 survey, 70% of young women surveyed agreed that girls are often bullied or harassed online and yet 44% do not feel comfortable reporting incidents of abusive online behaviour.¹² The Committee notes

⁸ Liam Hackett, *Cyberbullying and its Implications for Human Rights* (December 2016) UN Chronicle <<https://unchronicle.un.org/article/cyberbullying-and-its-implications-human-rights>>.

⁹ Australian Human Rights Commission, *Cyberbullying, Human Rights and Bystanders* <https://bullying.humanrights.gov.au/sites/default/files/content/pdf/bullying/VHB_cyberbullying.pdf>.

¹⁰ Brandwatch and Ditch the Label, 'Cyberbullying and Hate Speech: What can Social Data Tell us about Hate Speech Online?' (Report, 2016) <<http://www.ditchthelabel.org/research-papers/cyberbullying-and-hate-speech/>>.

¹¹ Azmina Chrodia, *Unsocial Media: The Real Toll of Online Abuse Against Women* (20 November 2017) Medium <<https://medium.com/amnesty-insights/unsocial-media-the-real-toll-of-online-abuse-against-women-37134ddab3f4>>.

¹² Plan International Australian and Our Watch, "'Don't Send Me That Pic': Australian Young Women and Girls Report Online Abuse and Harassment are Endemic' (Report, March 2016) 2 <<https://www.plan.org.au/-/media/plan/documents/reports/dont-send-me-that-pic.pdf>>.

that cyberbullying and online harassment and abuse of adolescents has been linked to lower self-esteem, poor school attendance and performance and, in some cases, increased depressive symptoms.¹³

Algorithm Discrimination

Information about individuals is collected by a growing number of third party sources and proliferation of Internet of Things devices, often without individuals being aware of the organisation or government agency that is collecting their information or what subsequently happens to it. Data collection underpins a growing data brokerage industry which involves accumulating data about individuals from various sources, combining it and either trading this information as a commodity or using this information to influence the behaviour of individuals. There is also a growing trend of using such data and algorithms in AI to make automated decisions. This leaves individuals with reduced bargaining power and threatens their right to freedom from discrimination because of the significant information and knowledge imbalances as they are not able to access let alone interpret or reflect on the data that their behaviour has generated. Further, more often than not, algorithms are powered by skewed input data, false logic or even the prejudices of their programmers.¹⁴

An example of skewed datasets is demonstrated in a study from the MIT and Stanford University researchers that found three commercial facial analysis programs powered by AI demonstrated significant error rates in determining the gender of any subject that was not white and male, given the datasets that underpin the algorithms are disproportionately focused on white men rather than other gender and racial types.¹⁵ A clear example of false logic or algorithmic bias is China's social credit system which has the potential to restrict the freedom of movement of and expression of dissidents.¹⁶ Further, big data gathered from the My Health Record could have the potential to predict cancer risk which, if inappropriately shared, could result in such data being used to influence insurance premiums.¹⁷

¹³ Sonja Perren et al, 'Bullying in School and Cyberspace: Associations with Depressive Symptoms in Swiss and Australian Adolescents' (2010) 4(28) *Child and Adolescent Psychiatry and Mental Health* 1 <<https://capmh.biomedcentral.com/articles/10.1186/1753-2000-4-28>>.

¹⁴ Daniel Cossins, *Discriminating algorithms: 5 times AI showed prejudice* (12 April 2018) New Scientist <<https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/>>.

¹⁵ Rich Hardy, *Study Finds Some Facial Recognition Systems Only Accurate for White Male Faces* (13 February 2018) New Atlas <<https://newatlas.com/racial-gender-bias-face-detection-software/53380/>>.

¹⁶ Matthew Carney, *Leave No Dark Corner* (18 September 2018) ABC News <<http://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278>>.

¹⁷ Ariel Bogle, *'Big Data' Says you're at Cancer Risk. Do you want your Insurer to Know? Do you want to Know?* (1 September 2018) ABC News <<http://www.abc.net.au/news/science/2018-09-01/health-data-growth-has-privacy-legal-implications/10156396>>.

Decent Work

In outlining internationally recognised human rights, the Issues Paper does not mention the "right to fair and productive employment and decent work", a pillar in the United Nations' plan to end poverty and one of the Sustainable Development Goals.¹⁸ The Committee submits that this right should be given due consideration as decent work is necessary for the preservation of human dignity given technology can have a dramatic effect on how people work, even making entire skill sets redundant.

New technology has led to the creation of new jobs and changed how other jobs are performed. It should be recognised that these changes in the employment landscape disproportionately affect low income earners. A clear example of this is Amazon's "no line, no check-out" store, Amazon Go, in a sector where job losses disproportionately impact women and people of colour.¹⁹ In the legal industry, many of the more formulaic tasks performed by junior lawyers and paralegals, such as discovery, have been disrupted by new technologies. As the Fourth Industrial Revolution continues, AI, robotics and other new technologies will lead to dramatic shifts within industries and cause disruption of economic power.²⁰ The Committee submits that the approach of government should include measures to mitigate disadvantage created by such change, and to assist workers in adapting to such change, such as consulting with workers and trade unions before and during the introduction of major technological change in the workplace.²¹ This will be necessary to minimise disruption to the economy and to ensure the right of all people to full and productive employment and decent work.

Dark Web

In outlining the different types of technology that raise human rights concerns, it is worth noting that particular groups of the community have resorted to the 'Dark Web' in an attempt to exercise and impede human rights. The Dark Web is an intentionally concealed layer of the Internet which is not indexed by mainstream search

¹⁸ *Transforming Our World: The 2030 Agenda for Sustainable Development*, GA Res 70/1, 70th sess, Agenda Items 15 and 116, Un Doc A/RES/70/1 (21 October 2015)

<http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E>.

¹⁹ Henry Grabar, *Amazon Go Is Dazzling. But How Many Jobs Will It Kill?* (22 January 2018) Slate

<<https://slate.com/business/2018/01/will-amazon-go-eliminate-cashier-jobs.html>>.

²⁰ Chris Pash, *The Australian Human Rights Commission Is Trying to Work out the Good and Evil of Technology* (24 July 2018) Business Insider Australia <<https://www.businessinsider.com.au/australia-human-rights-technology-2018-7#KUfB4Ltp7T0cX7uA.99>>.

²¹ Select Committee on the Future of Work and Workers, Department of the Senate, *Hope is not a Strategy – Our Shared Responsibility for the Future of Work and Workers* (2018)

<https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Future_of_Work_and_Workers/FutureofWork/Report>.

engines and only accessible through special software such as Tor (short for 'The Onion Router').²² Tor uses a distributed encryption model where Tor users' traffic is routed by the Tor network 'through a series of other users' computers [or relays] such that the traffic cannot be traced to the original user'.²³ Traffic is encrypted between relays (intended to echo the layers of an onion) and passes through at least three relays such that Tor users' IP addresses are thus, in theory, hidden.²⁴

The degree of anonymity provided to users of the Dark Web by the Tor network enhances the users' enjoyment of their right to privacy, especially in (in theory) frustrating attempts to conduct arbitrary, unlawful surveillance of users, for instance. This is especially beneficial for dissidents in countries that are governed by authoritarian regimes such as China.²⁵ This flows on to safeguarding Dark Web users' rights to thought and conscience, to 'hold opinions without interference', to expression, and to freely communicate and associate with others. This is because they can freely interact with fellow users without the risk of detection by government actors accompanying the use of non-Dark Web fora.

However, the Dark Web also invites criminal 'misuse' of human rights. Criminals could benefit from the privacy afforded since it enables them to evade law enforcement scrutiny. They can thus, at least in theory, freely organise and interact with each other in the digital underground on the Dark Web. The Dark Web has hosted many thriving marketplaces for all sorts of criminal goods, such as weapons, narcotics and cybercrime goods and services or indeed data stolen through the latter's usage.²⁶ Such is the scale of the problem that the shift by consumers from traditional street networks to illicit online marketplaces is considered to challenge established criminal business models.²⁷ The Dark Web is even considered to have reduced the barriers to entry for criminal entrepreneurs.²⁸ Furthermore, in response to seizures of illicit online markets by law enforcement agencies, the members of more sophisticated fora tend to undertake 'rigorous and aggressive vetting of [prospective members]' and transact 'on virtual private networks and darknets [the Dark Web], with

²² Giacomo Persi Paoli et al, 'Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web' (Report, RAND Corporation, 2017) 9 <https://www.rand.org/pubs/research_reports/RR2091.html>.

²³ Kristin Finklea, 'Dark Web' (Report, Congressional Research Service, United States Congress, 10 March 2017) 4 <<https://fas.org/srgp/crs/misc/R44101.pdf>>.

²⁴ Electronic Frontier Foundation, *What is a Tor Relay?* <<https://www.eff.org/pages/what-tor-relay>>.

²⁵ Finklea, above n 23, 8.

²⁶ Andy Greenberg, *Operation Bayonet: Inside the Sting that Hijacked an Entire Dark Web Drug Market* (8 March 2018) WIRED <<https://www.wired.com/story/hansa-dutch-police-sting-operation/>>; Joshua Bearman, *The Untold Story of Silk Road, Part 1* (23 May 2015) WIRED <https://www.wired.com/2015/04/silk-road-1/?mbid=social_fb>.

²⁷ Europol, 'European Union Serious and Organised Crime Threat Assessment: Crime in the Age of Technology' (Report, European Police Office, 2017) 22 <<https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>>.

²⁸ Lillian Ablon, Martin C. Libicki and Andrea A. Golay, 'Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar' (Report, RAND Corporation, 2014) x <https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf>.

anonymization and encryption capabilities enabled'.²⁹ The above factors arguably combine to threaten innocent citizens' enjoyment of their right to life in supporting criminal and/or terrorist activity.

Nonetheless, technologies like Tor that provide access to the Dark Web do not guarantee privacy and thus enjoyment of the other rights. The numerous successes of law enforcement agencies against illicit marketplaces — such as the Silk Road, AlphaBay and Hansa — on the Dark Web highlights the ability of agencies to de-anonymise users and take action against illegal communities in which criminal users organise themselves.³⁰ Conventional investigative techniques deployed against cybercrime can also be used in the Dark Web context. The FBI's investigation into the child pornography website, Playpen, deployed a network investigative technique in 2015 (as per a warrant) to discover roughly 1,300 IP addresses and trace them to individuals, resulting in criminal charges being filed against over 185 people.³¹

3. Australian Law Reform

It is evident that new technologies play an increasingly significant role in our lives. However, they also raise particular opportunities, risks and challenges. There is a need to strike an appropriate balance between new technologies and human rights, but also between competing human rights, in a digital era.

The Committee recognises the rapid pace of technological growth and considers it would be ineffective to only consider regulating specific new technology or sector specific technologies.³² For example, in the US health care sector, Software as a Medical Device (SaMD) has become a useful self-care tool. It is a digital technology that allows for the diagnosis of health conditions, and suggested treatments. SaMD has been regulated the same way any other medical device would be, however, the Food and Drug Administration has said that this approach is not “well-suited for the faster, iterative design, development, and type of validation used for software-based medical technologies.”³³

²⁹ Ibid.

³⁰ Greenberg, above n 26; Bearman, above n 26.

³¹ Finklea, above n 23, 8.

³² William D. Eggers, Mike Turley and Pankaj Kishnani, *The Future of Regulation: Principles for Regulating Emerging Technologies* (19 June 2018) Deloitte Insights <<https://www2.deloitte.com/insights/us/en/industry/public-sector/future-of-regulation/regulating-emerging-technology.html>>.

³³ Center for Devices and Radiological Health, 'Digital Health Innovation Action Plan' (Action Plan, US Food and Drug Administration, 2017) 2 <<https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf>>.

While specific legislation, regulation or codes of conduct and ethics³⁴ could be implemented in certain sectors, the human rights implications of new technology cannot be separated from a larger human rights framework. The Committee's preference on law reform is to focus on the human rights, which are less likely to be subject to drastic change and can encompass any new technology that is likely to be developed. In this regard, the Committee supports the establishment of a national human rights act or bill of rights, and a statutory right to privacy.

Bill of Rights

The Committee notes that Australia is now the only Western democracy without a bill of rights document.³⁵ The Committee suggests that the current era of technological development presents an opportunity to begin the process of developing a bill of rights. Australia could develop a human rights framework fully informed by the technological realities we are faced with and ensure all new technologies are developed with consideration of and in compliance with human rights.

The Committee also notes that although bills and legislative instruments are currently required to be assessed for compatibility with the rights and freedoms recognised in the seven core international human rights treaties to which Australia is a party, it is worth noting that a failure to comply with the statement of compatibility process will not affect the validity or operation of any act, meaning a finding that a proposed bill is incompatible with human rights will not necessarily prevent the bill from being passed through parliament.³⁶ It is hoped that the establishment of a bill of rights will overcome this shortfall and ensure all legislation, some of which may derogate human rights in an attempt to regulate new technologies, will uphold and remain consistent with our human rights.

Statutory Tort of Invasion of Privacy

³⁴ See, eg, Data Governance Australia, *Code of Practice* <http://datagovernanceaus.com.au/wp-content/uploads/2016/07/DGA_Code_of_Practice_2017_15.11.17.pdf>; Privacy Commissioner, *Principles for Safe and Effective Use of Data and Analytics*, NZ Government <<https://www.privacy.org.nz/assets/Uploads/Principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance3.pdf>>; UK House of Lords Select Committee on Artificial Intelligence, 'AI in the UK: Ready, Willing and Able?' (Report, 16 April 2017) <<https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/10002.htm>>; Institute of Electrical and Electronics Engineers, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems (EADv2)* <<https://ethicsinaction.ieee.org/>>; European Group on Ethics in Science and New Technologies, *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems* <https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf>.

³⁵ Australian Human Rights Commission, *Ten Common Questions about a Human Rights Act for Australia* <https://www.humanrights.gov.au/sites/default/files/content/letstalkaboutrights/downloads/HRA_questions.pdf>.

³⁶ *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth) s 8(5).

The Committee also notes that there has been a convergence across several common law jurisdictions regarding the need to recognize some form of a tort of invasion of privacy, such as in New Zealand,³⁷ the UK³⁸ and Canada.³⁹ Both the Australian Law Reform Commission⁴⁰ and the NSW Legislative Council's Standing Committee on Law and Justice⁴¹ have recommended a statutory cause of action where an individual can make a claim if they have suffered a serious invasion of privacy, in circumstances in which the person had a reasonable expectation of privacy. The Committee suggests that the infiltration of new technologies into individuals' lives gives significant impetus to introduce such a statutory tort of invasion of privacy, rather than continue to rely on other causes of action such as breach of confidence.

Guiding Principles

The Committee submits that any legislative or regulatory consideration should aim to maximise the effectiveness and accessibility of technology whilst limiting any negative human rights impacts. Professor Roger Brownsword prescribes three questions that should be asked when considering the adequacy of regulation: "whether regulation is *effective*, whether it is *legitimate*, and whether its *design* is optimal."⁴² The Committee considers this to be a sensible and practical approach and suggests five guiding principles in regulating new technologies.

Guiding Principle 1: Accountability

The Committee submits that many new technologies encompassing automated decision making and data aggregation obfuscate the capacity to identify who or what caused any human rights violations and should be held ultimately responsible. Due to the complexity and novelty of new technologies, there is a high likelihood that where technologies fail and result in harm to citizens, attribution of responsibility will often be difficult, and therefore time consuming and costly.

When regulating new technologies, a citizen's right and ability to obtain redress should be one of the key guiding principles for legislators and regulators. Legislators should ensure that they distribute the burden of

³⁷ *Hosking v Runting* [2005] 1 NZLR 1.

³⁸ *Douglas v Hello! Ltd* [2000] 2 WLR 992.

³⁹ *Privacy Act 1996 RSBC* c 373 (British Columbia); *Privacy Act CCSM* s P125 (Manitoba); *Privacy Act 1978 RSS* c P-24 (Saskatchewan); *Privacy Act 1990 RSNL* c P-22 (Newfoundland and Labrador).

⁴⁰ Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Vol 1, 339.

⁴¹ Parliament of NSW Standing Committee on Law and Justice, *Remedies for the Serious Invasions of Privacy in New South Wales*, Report No 57 (2016).

⁴² Roger Brownsword, 'What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity' in Roger Brownsword (eds), *Global Governance and the Quest for Justice - Volume IV: Human Rights* (Hart Publishing, 2004) 204 <<http://kavehh.com/my%20Document/KCL/Technology%20law/what%20the%20world%20needs%20now,%20techno-regulation%20human%20rights%20human%20dignity.pdf>>.

navigating legal complexity and uncertainty in a way that ensures the capacity of citizens to obtain redress is not reduced by that complexity and uncertainty. Legislative approaches that prioritise swift redress to an aggrieved party and subsequently allow an ultimate finding of responsibility are preferable when pre-empting potential harms that may flow from new technologies, subject to appropriate safeguards against abuse by litigants. Adopting fidelity funds, mandatory and sufficiently broad and clearly defined insurance requirements, statutory bodies such as the Australian Human Rights Commission with investigatory and enforcement powers, permission for and simplification of citizens private remedies are all means by which this can be achieved.

The Committee also submits that any legislative or regulatory consideration must be drafted with the principle of human dignity front-of-mind. Article 1 of the Universal Declaration of Human Rights states that “[a]ll human beings are born free and equal in dignity and rights”. The associated Covenants on Economic, Social and Cultural Rights, and Civil and Political Rights echo this sentiment. These documents provide the “essential ingredients of human dignity as empowerment.”⁴³ The preservation of human dignity must not be viewed as a constraint to the advancement of technology, but as a constant that must be considered and accommodated at every stage.

The Committee further submits that legislators and regulators should work closely with industry to, in advance of harms arising, proactively put in place efficacious review mechanisms which can be followed where an unexpected harm arises. Such mechanisms should, at the outset clearly identify an entity that is responsible for conducting the review, with any complexities around attribution of responsibility and costs being dealt with in parallel or after that review.

In this regard, it is worth noting that legislators should be prepared to regulate new technologies differently for children and young people as compared to adults, in order to properly mediate the rights and responsibilities of each group.

Guiding Principle 2: Transparency

The Committee submits that ensuring transparency, especially in relation to the reporting of events which negatively impact human rights ought to be at the forefront of legislators minds. Unless organisations are *required* to publicly disclose human rights violations, they have little or no incentive to inform a citizen, regulators or wider society of such violations. This is especially so where such a disclosure is likely to harm the bottom line or image of an organisation.

⁴³ Brownsword, above n 42, 211.

Considering the rapid pace at which many new technologies become pervasive, the Committee submits that swift reporting of incidents that can result in serious human rights violations is essential. While the benefits of adopting new technologies should not be understated, a failure to quickly articulate actual or potential human rights violations caused by new technologies erodes the perceived significance of human rights by inappropriately allowing organisations and technologies to retain legitimacy despite of their actions or inactions.

Additionally, appropriate transparency measures should be put in place to ensure that where an aggrieved party pursues compensation directly from an organisation in relation to a violation of their human rights because of a new technology, attempts to prevent dissemination of information relating to any violation, for example by making non-disclosure a requirement of an agreed settlement, can be rendered ineffectual by law. Such measures should only apply to the extent that the grievance is of a kind that is likely to have been experienced by others who may be unaware of the violation of their human rights.

Guiding Principle 3: Adaptability

Given the rapid pace of technology, particularly the adoption of technology which may have been inconceivable only a few years ago, means legislation and regulations may become outdated at a much quicker rate. The Committee submits that in acknowledgement of this reality, must come entrenched with ongoing mandatory review requirements, preferably by an independent body that is not directly subject to partisan political influence purposed with such enquiries and empowered to investigate concerns raised by the community in relation to new technologies. Legal provisions such as sunset clauses may be particularly relevant in the regulation of technologies which will foreseeably change so dramatically in the near future that the legislative framework that has been enacted will become redundant. Such clauses also ensure that human rights issues regarding technology have an opportunity to be reconsidered when such legislation is due to cease operating.

Guiding Principle 4: Accessibility

Notwithstanding the perhaps persisting notion that “[t]here are no real experts on the subject of regulating technologies”,⁴⁴ the Committee submits that new technologies must be able to be sufficiently understood by legislators, regulators and the wider public. There is a serious yet avoidable threat to human rights where legislators, regulators and the public are not privy to the implications that are known to those who are familiar

⁴⁴ Justice Michael Kirby, 'The Fundamental Problem of Regulating Technology' (Paper presented at the Conference on the Ethical Governance Of Information & Communications Technology and the Role of Professional Bodies, University House, Australian National University, 1 May 2008) 15 <http://www.hcourt.gov.au/assets/publications/speeches/former-justices/kirbyj/kirbyj_1may08.pdf>.

with the technology or which could have otherwise been discovered by conducting consultations with a wide range of stakeholders, including those able to bridge the gap between different kinds of relevant expertise.⁴⁵

The Committee submits that for this to occur, the process by which legislation is commissioned and drafted in consultation with technical experts should involve a cross-discipline of people who have a sufficient understanding of the technology, human rights and the law generally. To this end, it should be a key focus of government to upskill and incentivise retention of people who have technical expertise which relate to new technologies to further enable them to understand the law, human rights and how to share their technical expertise effectively.

Guiding Principle 5: Optimisation

In common law jurisdictions, new law is shaped and confined by older case law. In Australia, enacting statutes offers a means to bypass outdated common law but, as with the common law, older statutes often act as a scaffold for any future amendments or additions and therefore to an extent shape and confine future developments in law. While the Committee acknowledges that there are significant benefits in terms of certainty about what the law means when there is a history of interpretation to which to refer, in the context of new technologies, retrofitting old law with amendments or new provisions may be highly problematic and not result in a “fit for purpose” outcome.

The Committee submits that piecemeal amendment of statutes often makes the law difficult to navigate for the wider public and for all parties who have a stake in the legal system. Additionally, new statutes that are introduced over time may interact in unforeseen ways with older statutes, creating confusion and uncertainty. Because of this complexity *inter alia* navigating human rights implications is made more difficult which flows on to the ability of all stakeholders to voice concerns about human rights implications of technology in consideration of the current regulatory environment. Legislators should strive to create clear and concise legislation that is easy to navigate and more readily exercise their powers to overhaul difficult to navigate legislation or consolidate multiple pieces of legislation relevant to an industry or technology in the fewest number of legislative instruments possible.

Finally, the Committee submits that legislators and regulators must be informed by a broader appreciation of the context in which a specific technology is to be applied when contemplating how best to regulate any given technology. It is inadequate and detrimental to view technologies as in a vacuum and independent of one another as in many instances, it is not a single technology but a combination of different technologies which will give rise to detrimental human rights implications.

⁴⁵ Ibid 43.

4. Other Reforms

The Committee submits it is critical that educational tools and incentives accompany changes in technology which affects people with protected characteristics. For instance, children and young people, as well as their parents, caregivers and educators should be provided with extensive education and information about the risks relating to new technologies as well as their safe and responsible uses. To complement this, new technologies should have more stringent levels of safety and privacy for children and young people and better age and identity verification systems to assist with content filtering.

Similarly, education and information programs should also be provided to people of culturally and linguistically diverse backgrounds, older people and Aboriginal and Torres Strait Islander peoples, particularly in their language and community.

Finally, it is necessary to ensure greater awareness is brought to all individuals of their human rights, through training and educational programs provided by the Australian Human Rights Commission and the respective Commissioners for people with protected characteristics.

5. Concluding Comments

NSW Young Lawyers and the Committee thank you for the opportunity to make this submission. The Committee would appreciate further consultation on the Commission's proposals for change in its Discussion Paper.

Please note that the views and opinions expressed in this submission are on behalf of the Committee and its contributors and do not reflect the views or opinions of any employer or company related to the contributors.

If you have any queries or require further submissions, please contact the undersigned at your convenience.

Contact:

Alternate Contact:



David Turner
President
NSW Young Lawyers

Email: [Redacted]

Eva Lu
NSW Young Lawyers Communications, Entertainment
and Technology Law Committee

Email: [Redacted]