



THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: CLIC:DHas1712484

10 May 2019

Mr Jonathan Smithers
Chief Executive Officer
Law Council of Australia
DX 5719 Canberra

By email: sarah.sacher@lawcouncil.asn.au

Dear Mr Smithers,

Submission to the United Nations Committee on the Rights of the Child – Children’s Rights in Relation to the Digital Environment

Thank you for the opportunity to provide input to the Law Council’s submission to the United Nations Committee on the Rights of the Child (“the UN Committee”) regarding its proposed General Comment on Children’s Rights in Relation to the Digital Environment (“General Comment”).

The Law Society’s Children’s Legal Issues Committee and Human Rights Committee have contributed to this submission, which addresses some of the questions contained in the Concept Note for a General Comment on Children’s Rights in Relation to the Digital Environment prepared by the UN Committee (“the Concept Note”). As the UN Committee has set a short page limit for input, our submission is brief.

The purpose and scope of the General Comment

The Law Society supports the purpose of the proposed General Comment, as outlined in the Concept Note, to “clarify how [the] rapidly evolving [digital] environment impacts on the full range of children’s rights in positive and negative ways”. In the nearly three decades since the UN Convention on the Child (“UN CRC”) was adopted by the UN General Assembly in November 1989, there have been rapid advances in technology, with significant implications for children. Digital tools including tablets, smartphones, the internet and social media platforms are now interwoven into children’s daily lives,¹ and play a pivotal role in the way children learn, socialise and perceive the world. This trend towards increasing connectivity is continuing, so it is appropriate that the UN Committee develop guidance for States seeking to meet their obligations to promote and protect children’s rights in light of challenges and opportunities presented by the digital environment.

¹ Australian Communications and Media Authority, ‘Research snapshot: Aussie teens and kids online’ (05 February 2016). Available at: <https://www.acma.gov.au/theACMA/engage-blogs/engage-blogs/Research-snapshots/Aussie-teens-and-kids-online>

Addressing discrimination – both offline and online – to ensure all children have their rights realised in a digital world

A 2017 study by the Salvation Army surveyed 1,380 of their clients across Australia who accessed emergency relief, and found that 57% of children did not have access to the internet, and approximately one in three did not have access to a computer or tablet at home.² This follows a 2013 research study from the Smith Family which found that in Australia's most disadvantaged communities, only 68% of children aged 5 to 14 years accessed the internet at home over a 12 month period, compared to 91% of children in the most advantaged communities.³

In a 2017 submission to the UN Office of the High Commissioner for Human Rights ("UN OHCHR"), the Australian Government noted that children and adults in remote locations in Australia, "particularly in remote Indigenous communities" face problems accessing the internet.⁴ The UN Special Rapporteur on the right to freedom of opinion and expression has also highlighted disability as a factor in the 'digital divide', noting that persons with disabilities "often face barriers to accessing the Internet in a way that is meaningful, relevant and useful to them in their daily lives".⁵ With an increasing number of educational resources and communications tools requiring internet connectivity and digital literacy, there is a real risk that this digital divide will contribute to already-marginalised children missing out on new opportunities. This has potential implications for Australia's compliance with Article 29 of the UN CRC, which provides for a child's right to education directed to the development of their personality, talents and mental and physical abilities.

To address the impact of the digital divide on children, the Law Society recommends policymakers, businesses, and the education sector place a focus on improving internet connectivity for disadvantaged and marginalised communities, including children with disabilities. In this regard, we note that the Australian government has established a number of programs with the aim of improving internet availability and access for children and adults in remote regions, through the Indigenous Advancement Strategy. These initiatives have included support for 301 WiFi Telephone services in remote Indigenous communities, and funding for the Remote Indigenous Internet Training activity, which provides internet access, training and internet infrastructure in remote Indigenous communities to address barriers to access.⁶ We also note that the Australian Human Rights Commission has developed World Wide Web Access Advisory notes which provide guidance on the requirements for compliance with the *Disability Discrimination Act 1992* (Cth). The Advisory notes provide practical information on how to make websites more accessible to people with a disability, to assist them in accessing a wide range of often-critical information and services.⁷

Safety issues are another concern for young people, particularly young women, when they access the digital environment. A 2016 study by Plan International Australia and Our Watch found that seven out of ten Australian girls aged 15-19 believe online harassment and bullying is endemic, and 51% of girls believe that girls are pressured into taking explicit photographs of

² The Salvation Army, *The Hard Road: National Economics and Social Impact Survey 2017*, 7.

³ A Hampshire, 'Sport, culture and the internet: Are Australian children participating' (September 2013), presentation delivered at the Australian Social Policy Conference, Sydney. Available at: https://www.thesmithfamily.com.au/~media/files/research/policy-submissions/aspc_sport%20culture%20internet_sept13.ashx?la=en

⁴ Australian Government, Subject: Australian Response to OHCHR Questionnaire pursuant to HRC Resolution 32/13 (January 2017), File no 16/1163#18.

⁵ UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* (16 May 2011), Human Rights Council, 17th session, A/HRC/17/27, 61.

⁶ Ibid.

⁷ Australian Human Rights Commission, *World Wide Web Access: Disability Discrimination Act Advisory Notes ver 4.1* (2014). Available at: <https://www.humanrights.gov.au/our-work/disability-rights/world-wide-web-access-disability-discrimination-act-advisory-notes-ver>

themselves and sharing them.⁸ In a 2017 report, the UN OHCHR noted that “specific groups of women, in particular young women... may experience particularly severe forms of online violence” that impact on their human rights.⁹ Strategies to combat online violence against girls and women canvassed in the UN OHCHR report include legislation, education, preventative measures, and tools within software and social media platforms that promote safety and privacy.¹⁰

In Australia, the legislative response to online violence and harassment at the federal level has included the *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* (Cth), which supports the victims of ‘image-based abuse’ by providing the Office of the eSafety Commissioner with a range of enforcement options to require rapid removal of image-based abuse material and to hold perpetrators to account. Civil penalties under the Act range from \$105,000 for individuals to \$525,000 for corporations; perpetrators may also face penalties of imprisonment for up to five years under the *Criminal Code Act 1995* (Cth). The *Enhancing Online Safety Act 2015* (Cth), which established the office of the eSafety Commissioner, states at s 12 that the Commissioner “must as appropriate, have regard to the Convention on the Rights of the Child in the performance of [its] functions” in relation to Australian children.¹¹

In NSW, Division 15C of the *Crimes Act 1900* (NSW) contains offences for recording, distributing or threatening to distribute an intimate image without consent. In 2018, the NSW Parliament passed the *Crimes (Domestic and Personal Violence) Amendment Bill 2018* (NSW), which amends the definitions of ‘stalking’ and ‘intimidation’ in the *Crimes (Domestic and Personal Violence) Act 2007* (NSW) to specify that these terms cover activities conducted online or via text messages that are designed to instill fear of physical or mental harm. A note in the legislation explains that this expanded definition is designed to cover the bullying of a person by email or social media.¹²

To ensure these legislative responses meet their aim, and effectively protect the safety of young people online, the Law Society submits that it is important for children to have access to advocates who can act on their behalf and provide advice on their options. Young people who bring forward a complaint in relation to online harassment should always be treated seriously, and with respect.

How can States better realise their obligations to children’s rights in relation to the digital environment?

Protecting children’s right to privacy in the digital environment

The right to privacy is recognised as a fundamental human right in the *Universal Declaration of Human Rights*, the *International Covenant on Civil and Political Rights* and the UN CRC.

The UN CRC provides at Article 16 for a child’s right to privacy in the following terms:

1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.

⁸ Plan International Australia and Our Watch, “Don’t send me that pic”: Australian Young Women and girls report online abuse and harassment are endemic (Melbourne: Plan International Australia, 2016), 2.

⁹ UN General Assembly, *Promotion, protection and enjoyment of human rights on the Internet: ways to bridge the gender digital divide from a human rights perspective: Report of the United Nations High Commissioner for Human Rights* (5 May 2017), UN Human Rights Council, 35th session, 36.

¹⁰ *Ibid.* 37.

¹¹ *Enhancing Online Safety Act 2015* (Cth), s12.

¹² *Crimes (Domestic and Personal Violence) Amendment Act 2018* (NSW), s 7(1)(a).

2. The child has the right to the protection of the law against such interference or attacks.

In its 2014 report, *Serious Invasions of Privacy in the Digital Era*, the Australian Law Reform Commission (“ALRC”) stated that “education about privacy risks and management may be particularly important for children and young persons.”¹³ In support of this statement, the ALRC cited research indicating that the use of privacy settings on social media is higher among older Australians. The ALRC suggested “privacy awareness campaigns and other strategies targeted at younger Australians” as a means of protecting children’s right to privacy in the digital environment.

In addition to awareness campaigns on the right to privacy, the Law Society continues to support the recommendation of the ALRC that a new Commonwealth Act enact a statutory cause of action for serious invasion of privacy.¹⁴ In particular, the Law Society endorses the ALRC’s recommendation that the new tort should cover two types of invasion of privacy: intrusion upon seclusion; and misuse of private information. As the ALRC recommended in 2014, the design of legal privacy protection should be “sufficiently flexible to adapt to rapidly changing technologies and capabilities, without needing constant amendments”.¹⁵ This recommendation is particularly salient in light of the exponential pace at which new technologies such as AI and blockchain are developing, and the evolving scope of their application.

A principles-based approach to protecting human rights in the digital environment

The Law Society has previously recommended that any legislation protecting human rights in respect of new technologies be principles-based, to allow for flexibility and adaptability. This approach should also be followed when developing legislation to protect and promote the rights of children in the digital environment. The principles that the Law Society believes should guide legislation in this area are fairness, transparency, non-discrimination and accountability. For a description of how these principles could be applied in practice, please see our **attached** submission dated 14 September 2018 relating to the Australian Human Rights Commission consultation on human rights and technology.

How should the practices of business operating in the digital environment support the realisation of children’s rights?

Companies that create and operate digital technologies have a responsibility to respect and promote the rights of all people who access their technology, including children. These responsibilities are articulated by the UN Guiding Principles on Business and Human Rights (“UNGPs”) which were endorsed by the UN Human Rights Council in 2011. Under the UNGPs, companies are expected to respect human rights and avoid causing adverse human rights impacts through their activities. The UNGPs recommend that companies ensure compliance with this responsibility to respect human rights through:

- Expressing their commitment through a statement of policy;
- Implementing effective human rights due diligence to identify, prevent and address actual or potential human rights impacts;
- Mainstreaming human rights consideration across business operations and activities based on that due diligence; and

¹³ Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014), 40.

¹⁴ See

<https://www.parliament.nsw.gov.au/lcdocs/submissions/51194/0015%20The%20Law%20Society%20of%20New%20South%20Wales%20.pdf>

¹⁵ Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014), 36.

- Enabling access to effective grievance mechanisms by affected groups and individuals.¹⁶

The UNGPs also require States to provide effective guidance to business enterprises on how to respect human rights throughout their operations. To spur action within the technology sector, we recommend that the Commonwealth Government develop and update guidance for businesses on supporting the realisation of children's rights in the digital environment.

We also recommend that businesses proactively consider user safety in the design of digital products, particularly where the product is likely to be used by children and young people, to ensure the child is protected from violence and abuse online. In this regard we note the *National Principles for Child Safe Organisations*, which were endorsed by the Council of Australian Governments, including the Prime Minister and state and territory First Ministers, in February 2019. Principle eight requires that “[p]hysical and online environments promote safety and wellbeing while minimising the opportunity for children and young people to be harmed”, and includes a number of action areas for organisations to follow.¹⁷

Thank you for the opportunity to provide input on this topic. Should you have any questions or require further information, please contact Andrew Small, Policy Lawyer on (02) 9926 0252 or email andrew.small@lawsociety.com.au.

Yours sincerely,

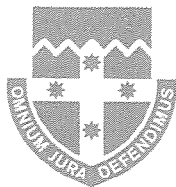


Elizabeth Espinosa
President

Enc.

¹⁶ United Nations, *Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework* (2011) HR/PUB/11/04

¹⁷ Australian Human Rights Commission, *National Principles for Child Safe Organisations*, (2019). Available at: <https://www.humanrights.gov.au/sites/default/files/National%20Principles%20for%20Child%20Safe%20Organisations.pdf>



THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: HRC/DHas: 1581980

14 September 2018

Mr Jonathan Smithers
Chief Executive Officer
Law Council of Australia
DX 5719 Canberra

By email: nathan.macdonald@lawcouncil.asn.au

Dear Mr Smithers,

Consultation on Human Rights and Technology

Thank you for the opportunity to provide input to a potential Law Council of Australia submission to the Australian Human Rights Commission ("AHRC") consultation on human rights and technology.

This submission is informed by our Human Rights Committee and our Privacy and Data Law Committee.

The human rights impact of new technologies: our focus in this submission

New technologies¹ such as Artificial Intelligence ("AI"), robotics, the Internet of Things, and virtual reality have the potential to both promote and imperil human rights. The Issues Paper on Human Rights and Technology ("Issues Paper") published by the AHRC in July 2018 identifies a suite of human rights that new technologies might affect, from the right to education, to the right to a fair trial, to the right to benefit from scientific progress. In this submission, the Law Society focuses primarily on the implications that new technologies hold for the right to privacy, the right to equality and non-discrimination, and the right to accessibility.

New technologies and marginalised groups in Australia

The Issues Paper published by the AHRC observes that "specific groups will feel both the positive and negative impacts of new technologies differently to other Australians".² At the level of access, this trend can be seen in the digital divide affecting many groups across Australia. The 2017 Australian Digital Inclusion Index found that several groups are particularly digitally excluded: people in low income households, people aged 65 and over, people with a disability, people who did not complete secondary school, Indigenous

¹ In this submission, the Law Society of NSW uses the term "new technologies" as shorthand for the 12 types of technology highlighted at page 18 of the Issues Paper published by the AHRC, namely: new computing technologies; blockchain and distributed ledger technologies; the Internet of Things; AI and robotics; advanced materials; additive manufacturing and multidimensional printing; biotechnologies; neurotechnologies; virtual reality and augmented reality; energy capture, storage and transmission; geoen지니어ing; and space technologies.

² Australian Human Rights Commission, *Human Rights and Technology Issues Paper* (2018) 20.

THE LAW SOCIETY OF NEW SOUTH WALES

170 Phillip Street, Sydney NSW 2000, DX 362 Sydney
ACN 000 000 699 ABN 98 696 304 966

T +61 2 9926 9333 F +61 2 9231 5809
www.lawsociety.com.au



Law Council
OF AUSTRALIA
CONSTITUENT BODY

Australians, and people not in paid employment. Women in Australia are also less likely to be online than men, particularly those in the 65 and over age group.³

With an increasing number of jobs, social services and communications tools requiring internet connectivity and digital literacy, there is a real risk that this digital divide will contribute to already-marginalised groups missing out on new opportunities. To address this trend, policymakers, businesses, and the education sector should place a focus on improving the digital ability of people in marginalised groups, as well as addressing the affordability and accessibility of digital tools.

How should Australian law protect human rights in the context of AI informed decision-making

In an article published in *Science* in August 2018, Mariarosaria Taddeo and Luciano Floridi of the University of Oxford described AI as “a powerful force that is reshaping daily practices, personal and professional interactions, and environments”.⁴ As AI systems become more tightly woven into everyday life – from the household to the government level – the risk of AI informed decision-making having a negative impact on human rights grows. The Law Society notes that the continued rise of AI across many systems in everyday life has the potential to effectively institutionalise discrimination, diminishing accountability in relation to the making of AI informed decisions. As the Issues Paper notes, instances of unjust consequences arising from AI informed decision-making have already occurred internationally in areas including recruitment, performance management and issuance of bail.⁵ Unless guidelines and regulation are introduced to ensure fairness, transparency and accountability of algorithmic decision-making, the complexity, intricacy and inscrutability of these systems could compound disadvantage for some sectors of the community.

We note that the EU Fundamental Rights Agency stated in a 2018 report that if AI informed decision-making models are informed by biased data or algorithms, “discrimination will be replicated, perpetuated and potentially even reinforced”.⁶ We also note that in a report published in April 2018, the UK House of Lords Select Committee on Artificial Intelligence stated that “the prejudices of the past must not be unwittingly built into automated systems, and such systems must be carefully designed from the beginning.”⁷

The Law Society submits that fairness, transparency, non-discrimination and accountability should be the central focus of regulation in the area of AI so as to prevent inequality from becoming further entrenched within social, governmental and economic systems. The Law Society supports the establishment of appropriately regulated AI-informed decision-making processes which will allow for the benefits of AI to be provided to society while protecting fundamental rights, including the rights to privacy⁸ and non-discrimination.⁹

The Law Society agrees with the position in the Issues Paper that robust and transparent procedures and guidelines are necessary regulatory steps to maximise the benefits and minimise the risks of AI in Australia. In particular, we note the importance of increased

³ Julian Thomas et al, *Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2017* (RMIT University, 2017) 5.

⁴ Mariarosaria Taddeo and Luciano Floridi, 'How AI can be a force for good' (2018) 361(6404) *Science* 751.

⁵ Australian Human Rights Commission, above n 2, 30.

⁶ European Union Agency for Fundamental Rights, *#BigData: Discrimination in data-supported decision-making* (FRA Focus, 2018) 10.

⁷ House of Lords of the United Kingdom Select Committee on Artificial Intelligence, *AI in the UK: ready, willing and able?* (House of Lords, 2018) 5.

⁸ *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.

⁹ *Ibid*, art 24.

transparency as a guiding principle, which will work to equip the public with necessary information to prevent harm, as well as empower individuals to better comprehend, assess and query decisions made by AI systems. In this regard, the Law Society is of the view that members of the public should be aware of how and when AI systems are being used to make decisions about them, and the implications this will have.

The principles that should be applied to protect human rights in respect of new technologies

The Law Society considers that the best approach to the development of legislation in this area is for laws to be principles-based, which will allow for flexibility and adaptability. As noted above, the principles that we believe should guide legislation in this area are: fairness, transparency, non-discrimination, and accountability. In practice, these principles would require that, for example:

- *Fairness.* Organisations must only collect data on a person for a legitimate purpose, and consider reasonable community expectations relating to the collection of this data.
- *Transparency.* An organisation must act with transparency when collecting, using and disclosing personal information, and disclose any use of data in an intelligible format. This should include the opportunity for individuals to correct records and to withdraw information. Furthermore, when AI informed decision-making has the potential to impinge on human rights, the source code that is the basis of these decisions should be open for public scrutiny.
- *Non-discrimination.* All algorithms that are used to make decisions about individuals must be evaluated for discriminatory effects, preferably prior to roll-out and on a periodic basis.
- *Accountability.* There must always be a line of responsibility for business and government actions to establish who is accountable for consequences arising from the use of new technologies.

Gaps in existing Australian legislation regulating the use of AI and related technologies

The Law Society submits that the current legal framework for AI is inadequate and insufficient to protect human rights, and we consider recent issues relating to the adoption of AI around the globe highlight the potential for the utilisation of AI to create a complex web of legal, ethical and societal problems.

The Law Society supports the introduction of robust legal and regulatory guidelines to:

- regulate how AI algorithms are developed;
- regulate the areas where AI can be utilised in conjunction or in substitution for human expertise and labour; and
- establish effective monitoring and accountability measures to better identify, control and respond to AI issues.

The Law Society considers that the significant pace of change in this area will create challenges for the appropriate, timely and adequate development of robust measures, however we submit that it is essential for such measures to be developed noting the major changes that new technologies such as AI will have on the legal and economic landscape.

Protecting the right to privacy in an era of new technology

The Law Society is of the view that laws protecting individuals against breach of privacy have not kept pace with technological developments, and should be reviewed and reformed. New technologies, such as those that enable corporations and governments to build up detailed profiles of individuals based on their personal data and browsing history, present an unprecedented scope for serious invasions of privacy. The right to privacy is recognised as a fundamental human right in the *Universal Declaration of Human Rights*, the *International Covenant on Civil and Political Rights* ("ICCPR"), the *Convention on the Rights of the Child* ("CRC") and other instruments and treaties.

Article 17 of the ICCPR states:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.¹⁰

Article 16 of the CRC is in similar terms in relation to children.

Australia's obligations under the ICCPR and CRC – which Australia ratified in 1980 and 1990 respectively – require enhanced protections against breach of privacy, to protect against incursions of privacy enabled by new technologies. The 2014 Australian Law Reform Commission ("ALRC") inquiry into Serious Invasions of Privacy in the Digital Era at Recommendation 5-1 and 5-2 outlined how the current gap in privacy legislation could be addressed. The Law Society continues to support the recommendation of the ALRC that a new Commonwealth Act enact a statutory cause of action for serious invasion of privacy.¹¹ In particular, the Law Society endorses the ALRC's recommendation that the new tort should cover two types of invasion of privacy: intrusion upon seclusion; and misuse of private information.¹²

As the ALRC recommended in 2014, the design of legal privacy protection should be "sufficiently flexible to adapt to rapidly changing technologies and capabilities, without needing constant amendments".¹³ This recommendation is particularly salient in light of the exponential pace at which new technologies such as AI and blockchain are developing, and the evolving scope of their application.

Regulating new technologies: lessons to learn from international human rights law and other countries

States and regional bodies across the world are grappling with similar problems of how to apply existing legislation to new technologies, and how to develop new regulations to address the gaps that emerge. In the European Union, Article 22 of the General Data Protection Regulation ("GDPR") contains rules to protect individuals in the context of automated decision-making with a legal or otherwise significant effect on them. The Law

¹⁰ *International Covenant on Civil and Political Rights*, above n 8, art 17.

¹¹ See:

<https://www.parliament.nsw.gov.au/lcdocs/submissions/51194/0015%20The%20Law%20Society%20of%20New%20South%20Wales%20.pdf>

¹² Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014), 9.

¹³ Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014), 36.

Society is of the view that provisions in the GDPR protecting individual rights in the face of AI-informed decision making, as well as regulating the type of data that can be used, are a benchmark for how these issues should be approached.

The Law Society encourages the AHRC, along with government at the state and federal level in Australia, to continue to learn from international best practice in the regulation of new technologies. We therefore support the ongoing partnership between the AHRC and the World Economic Forum, and await the White Paper that will result in early 2019.

The role and responsibilities of technology companies in respecting human rights

In addition to the role of government in regulating new technologies, companies that are creating and operating new technologies have their own responsibility to respect human rights. These responsibilities are articulated by the UN Guiding Principles for Business and Human Rights (“UNGPs”), which were endorsed by the UN Human Rights Council in 2011. Under the UNGPs companies are expected to respect human rights and avoid causing adverse human rights impacts through their activities. The UNGPs recommend that companies ensure compliance with this responsibility to respect human rights through:

- expressing their commitment through a statement of policy;
- implementing effective human rights due diligence to identify, prevent and address actual or potential human rights impacts;
- mainstreaming human rights consideration across business operations and activities based on that due diligence; and
- enabling access to effective grievance mechanisms by affected groups and individuals.¹⁴

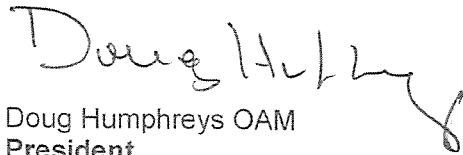
To maximise the potential benefits that new technologies hold for human rights, while minimising the risks, the Law Society recommends that technology companies operating in Australia follow the UNGP steps outlined above. To spur action within the private sector, we recommend that the Commonwealth Government develop guidance for businesses on conducting effective human rights due diligence in accordance with the UNGPs. The Law Society also recommends that the Government continue reform of the National Contact Point for the OECD Guidelines on Multinational Enterprises to ensure additional resources for joint fact-finding, improved mediation services and determination of grievances where relevant.

In recognition of the important role that companies have to play in this area, we recommend that the AHRC build a focus on the human rights responsibilities of companies as it implements its project on human rights and technology. We also encourage the AHRC to consult with experts on business and human rights, both within Australia and internationally, to inform their consideration of these important issues.

¹⁴ *United Nations, Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework* (2011) HR/PUB/11/04

Thank you for the opportunity to provide input on this topic. Should you have any questions or require further information please contact Andrew Small, Policy Lawyer, on (02) 9926 0252 or email andrew.small@lawsociety.com.au.

Yours sincerely,

A handwritten signature in black ink that reads "Doug Humphreys". The signature is written in a cursive style with a long, sweeping tail on the final letter.

Doug Humphreys OAM
President