

La Trobe Law Tech Submission

**To the Australian Human Rights Commission's
Technology and Human Rights Issue Paper**

Email: tech@humanrights.gov.au

2 October 2018

Human Rights Commissioner

Human Rights and Technology Project

Australian Human Rights Commission.

Level 3, 175 Pitt Street

Sydney NSW 200.

Dear Mr Santow,

Re: Human Rights and Technology: Issues Paper (2018)

La Trobe LawTech appreciates to opportunity to provide responses to the Australian Human Rights Commission's issues paper entitled Human Rights and Technology.

La Trobe LawTech (<https://www.latrobe.edu.au/law/la-trobe-law-tech>), based at the La Trobe Law School, was formed in 2017 by a multidisciplinary group of scholars working nationally and internationally on different aspects of data technologies, law and society.

We appreciate the Commission's recognition of the fact that technologies may be used to advance or undermine human rights. We urge the Commission to deepen its analysis of the conditions under which data technologies may support human rights in Australia and to consider the role that the Commission and other bodies can play to strengthen such use of technologies.

In this brief submission we illustrate aspects of such usage with reference to:

- a) Access to justice, especially by supporting the more efficient operation of courts;
- b) Preventing racial vilification on social media platforms; and
- c) Assurance that state actions comply with the law, by employing Compliance by Design.

We conclude with observations on appropriate governance and management of data technologies and internet access, information access and privacy.

1 Technology and Access to Justice

An inaccessible justice system heightens existing economic, cultural and social inequalities and vulnerabilities within society. The prohibitive cost of private legal services means that a growing number of Australians are falling into the ‘justice gap’, where they cannot afford a lawyer but are ineligible for legal aid or pro bono legal services. Supporting this, the Law and Justice Foundation of New South Wales’ Legal Australia-Wide Survey on Legal Needs in Australia found that only 51 per cent of respondents sought advice for a legal problem, 31 per cent handled legal problems without advice, and 18 per cent took no action at all for legal problems¹. This is not equal justice under the law for all Australians.

The convergence of innovative NewLaw business models and technology is helping to fill the justice gap by increasing efficiencies, providing price certainty and offering a more flexible, transparent and client-centric alternative to BigLaw².

While NewLaw firms are achieving better and more cost-effective outcomes for both lawyers and clients³, disruption within the legal services market is slow to evolve⁴. This is, in part, due to a profession that is typically risk averse, technologically illiterate, dominated by rigid ownership structures and interested in short-term profits. However, the incremental change is also due to the highly regulated nature of the legal profession.

In Australia, lawyers hold a monopoly over the practise of law and the provision of ‘legal advice’, thus restricting the level of competition and pace of disruption that would otherwise be possible. Whilst it is important to ensure certain standards and protections for the public, the burdening and potentially anti-competitive effect of regulation on innovation must also be considered.

Reforms to professional regulation are warranted to ensure that in an age of technological advancements, regulation does not become in and of itself an outdated barrier to access to justice.

¹ Christine Coumarelos et al, ‘Legal Australia-Wide Survey: Legal Needs in Australia’ (Survey, Law and Justice Foundation of New South Wales, August 2012) xvii.

² Traditional legal business models are commonly known as BigLaw business models. In contrast, NewLaw business models are the antithesis to BigLaw business models in that they represent a significantly different approach to the provision of legal services through using different models, processes or tools (e.g., fixed-fee virtual firms).

³ Emma Ryan, *BigLaw ‘rapidly’ losing out to NewLaw counterparts* (20 February 2017)

<[https://www.lawyersweekly.com.au/newLaw/20562-biglaw-rapidly-losing-out-to-newLaw-counterparts](https://www.lawyersweekly.com.au/newlaw/20562-biglaw-rapidly-losing-out-to-newlaw-counterparts)>.

⁴ Katie Miller, ‘Disruption, Innovation and Change: The Future of the Legal Profession’ (Report, Law Institute of Victoria, December 2015) 28 <<https://www.liv.asn.au/Flipbooks/Disruption--Innovation-and-Change--The-Future-of-t.aspx>>.

In particular, the question of what constitutes ‘legal work’ is currently a vexed question. This lack of clarity creates regulatory barriers that discourage new legal delivery models and innovative technological solutions to the justice crisis. If the fundamentals of what is considered ‘legal work’ is reconsidered, reconceptualised and defined in light of technological advancements, the cost of legal services is likely to decrease, which in turn would increase access to justice for all Australians.

2 Technology and the Courts

To date, much of the discussion about the potential use of so-called artificial intelligence (AI) tools in courts, particularly in Europe and the USA, has focussed on their potential to replace judicial-decision-making. Given the current state of the technology, this is largely a distraction. Currently, assisted decision-making tools do offer the potential to streamline the handling of some relatively straightforward types of court caseloads, for example, strict liability traffic or revenue offences where there are standardised non-custodial penalties with little or no room for discretionary application. However, much of the work done by judges and courts is a great deal more complex – requiring the court to first find the facts before attempting to adjudicate - and carries with it the responsibility to ensure a fair trial. At the present time, these tasks and that responsibility are not capable of being reduced to automated processes. If and when that occurs, it will be necessary to decide to what extent we as a community would be comfortable with them being carried out by automated processes.

Currently AI tools, such as assisted decision-making, do however hold a promise of enhancing access to justice by assisting individuals with legal problems to navigate court and tribunal processes and resolve legal disputes at an earlier stage. For example, the Canadian Civil Resolution Tribunal, Canada’s first online tribunal, requires parties seeking to use its dispute resolution process to first engage with its ‘Solution Explorer’ application. This is a relatively simple system in which the person is asked a series of ‘diagnostic’ questions that allows Solutions Explorer to offer them targeted information relevant to their problem. Solution Explorer assists the person to make an informed decision as to how to proceed and provides tools to help them implement their decision. These types of systems could also have application to assist in providing information and support to defendants, victims and witnesses in criminal cases.

Assisted-decision making tools do carry with them the potential for in-built bias – for example, they can be designed to steer individuals to particular solutions by not giving them full information about their rights. So, for example, a defendant charged with a minor traffic offence might not be aware

that they can still choose to have ‘their day in court’, if all the information that they receive is designed to discourage them from taking that course.

The risk of bias in algorithmic analysis that is used, for example, to inform decisions about penalties or release on bail, has been a source of controversy, as the discussion paper identifies (p.29)..

However, while that risk should not be minimised, there is also potential for properly-constructed algorithms to identify and mitigate the risk of bias that can exist in human decision-making. The risk of ‘unconscious bias’ has been highlighted by senior judicial officers as something that judicial decision-makers need to guard against⁵ and algorithms could provide a useful tool to assist judges to ‘bias check’ their decisions on matters such as bail and penalty.

Work is being done in Europe under the auspices of European Commission for the Efficiency of Justice (CEPEJ) to develop a European Ethical Charter on the use of artificial intelligence in judicial systems.⁶ The Commission might wish to closely examine its draft recommendations, which are due to be finalised later in 2018..

3 Racial vilification and freedom of speech

The impact of new digital communications technologies is particularly noticeable in the area of racial vilification. Social media platforms have provided abusers with access to a global audience and the capability to take racism viral. Meme generators and other online utilities have enabled the creation and propagation of new and powerful forms of racist content. In some cases, access to the profiles of social media users, accompanied by the deployment of advanced data analytics, has permitted racist content to be micro-targeted. Fraudulent social media accounts, created with relative ease, can make it difficult for law enforcement, national security and human rights bodies to attribute responsibility for racist content including content that incites violent extremism. These factors may

⁵ Chief Justice Beverley McLachlin, ‘Judicial Impartiality: The Impossible Quest?’ in Ruth Sheard (ed), *A Matter of Judgment: Judicial decision-making and judgment writing* (Judicial Commission of New South Wales, 2003) 15, 21-3; Justice Keith Mason ‘Unconscious Judicial Prejudice’ in Ruth Sheard (ed), *A Matter of Judgment: Judicial decision-making and judgment writing* (Judicial Commission of New South Wales, 2003) 27, 29-30.

⁶ Council of Europe European Commission for the efficiency of justice (CEPEJ), ‘The use of artificial intelligence (AI) in judicial systems at the heart of the discussions of the CEPEJ Working Group on Quality of Justice,’ (14 September 2018) at <https://www.coe.int/en/web/cepej/home/-/asset_publisher/NypRXgVwMdvN/content/the-use-of-artificial-intelligence-ai-in-judicial-systems-at-the-heart-of-the-discussions-of-the-cepej-working-group-on-quality-of-justice?_101_INSTANCE_NypRXgVwMdvN_viewMode=view/>.

require not only new approaches when compared to efforts tackling off-line racism, but also consideration of different legal doctrine.⁷

An examination of whether Commonwealth, State and Territory anti-discrimination laws are properly adapted to our new digital communication environment, whether regulators have sufficient powers and remedies to undertake their functions in this new environment and the desirability of developing public policy approaches in addition to legal and regulatory responses would be helpful. The work of Cyber-Racism and Community Resilience project may provide a significant start on this work and could be reviewed within the scope of the Human Rights and Technology project.⁸

Social media platforms must have some responsibility and accountability for content on their platform. Germany supports this approach through regulation and fines of up to €50 million for non-complying social media companies.⁹ The UK is currently considering a similar approach.¹⁰ The European Union uses co-regulation with a Code of Conduct agreed with platforms and monitored for compliance.¹¹ The United States opposes this approach and has sought to create safe harbours to protect technology platforms.¹² In Australia, the *Enhancing Online Safety Act 2015* (Cth) gives effective regulator powers to the e-Safety Commissioner, but doesn't cover cyber-racism. The scheme could be extended or serve as a model to enable regulation by the AHRC.¹³

Social media content published in Australia must comply with Australian laws and take account of the Australian context. This requires local knowledge. Companies should be encouraged to employ Australia staff, engage with all levels of government and with a broad cross section of Australian civil society and business. Past failures in this regard include platforms' difficulty understanding Aboriginal memes referencing petrol as racist commentary on substance abuse.¹⁴ Another example

⁷ Andre Oboler, 'Legal Doctrines Applied to Online Hate Speech' (2014) 87 *Computer and Law* <<http://www.austlii.edu.au/au/journals/ANZCompuLawJl/2014/4.pdf>>.

⁸ CRaCR Team, *Cyber Racism and Community Resilience: Project Report and Recommendations to the Australian Human Rights Commission* (June 2017)

⁹ Natasha Lomas, 'Germany's social media hate speech law is now in effect', *TechCrunch* (online), 2 October 2017 <<https://techcrunch.com/2017/10/02/germanys-social-media-hate-speech-law-is-now-in-effect/>>.

¹⁰ Charles Hymas, 'Government draws up plans for social media regulator following Telegraph campaign', *The Telegraph* (online), 20 September 2018 <<https://www.telegraph.co.uk/news/2018/09/20/government-draws-plans-social-media-regulator-following-telegraph/>>.

¹¹ European Commission, *Countering illegal hate speech online – Commission initiative shows continued improvement, further platforms join* (19 January 2018) <http://europa.eu/rapid/press-release_IP-18-261_en.htm>

¹² Josh Wingrove and Ben Brody, 'Trump Wants NAFTA to Limit Liability of Internet Firms Including Google, Facebook', *Insurance Journal* (online), 27 November 2017 <<https://www.insurancejournal.com/news/national/2017/11/27/472192.htm>>.

¹³ Gail Mason and Natalie Czapski, 'Regulating Cyber-Racism' (2017) 41(1) *Melbourne University Law Review* 284, 337-338.

¹⁴ Andre Oboler, *Aboriginal Memes and Online Hate* (Online Hate Prevention Institute, 2012) 13. <<http://ohpi.org.au/reports/IR12-2-Aboriginal-Memes.pdf>>.

is that Australia's long-standing position on online Holocaust denial as unlawful,¹⁵ is largely ignored by Facebook. The company applies its own global policy which opposes removal of such content and instead 'recognize[s] people's right to be factually wrong about historical events'.¹⁶ In contrast, In Germany, Facebook now employs local moderators and applies local law after significant pressure including law reform.¹⁷

Online racial vilification is not a problem that can simply be delegated to regulators. It must involve cooperation between a range of stakeholders with different capabilities.¹⁸ Implementing this approach requires the use of a flexible cocktail of public policy instruments including funding, education and training and ongoing dialogue. This should include support for civil society organisations to cope with new problems resulting from technological change, as well as support for new and innovative civil society organisations and responses that emerge to tackle emerging problems. Civil society is often excluded from innovation funding created for business,¹⁹ and there is no equivalent support for innovation that will enhance human rights rather than generating a commercial return. Australian innovation in this space has been at the leading edge globally,²⁰ but is stifled by this lack of support.

Addressing the impact of technology empowered racial vilification, and the potential impact of technological approaches to this problem, will be increasingly important to the core work of the AHRC.

4 Compliance by Design and Compliance through Design

Increasingly complex decision-making and actions by government require sophisticated governance and management controls to prevent actions in contraventions of law, procedures and policies,

¹⁵ *Toben v Jones* [2003] FCAFC 137

¹⁶ Richard Allan, e-mail of 29 August 2011 in Andre Oboler and David Matas, *Online Antisemitism: A systematic review of the problem, the response and the need for change* (Israeli Foreign Ministry, 2013) 50 <<http://mfa.gov.il/mfa/abouttheministry/conferences-seminars/gfca2013/documents/onlineantisemitism.pdf>>; Sam Levin, 'Zuckerberg defends Facebook users' right to be wrong – even Holocaust deniers' *The Guardian* (online), 19 July 2018 <<https://www.theguardian.com/technology/2018/jul/18/zuckerberg-facebook-holocaust-deniers-censorship>>.

¹⁷ Linda Kinstler, 'Can Germany Fix Facebook?', *The Atlantic* (online), 2 November 2017 <<https://www.theatlantic.com/international/archive/2017/11/germany-facebook/543258/>>.

¹⁸ Andre Oboler and Karen Connelly, 'Building SMARTER Communities of Resistance and Solidarity' (2018) 10(2) *Cosmopolitan Civil Societies: An Interdisciplinary Journal* <<https://epress.lib.uts.edu.au/journals/index.php/mcs/article/view/6035/6475>>.

¹⁹ Department of Industry Innovation and Science, 'Entrepreneurs' Programme - Programme Guidelines Version 9' (2017) Cl 100(a) <<https://www.business.gov.au/-/media/Business/EP/Entrepreneurs-Programme-Guidelines-pdf.pdf?la=en&hash=B0604206A0F72C232F0EDE9B9B92BA45766BED2C>>.

²⁰ Gagliardone, I., Gal, D., Alves Pinto, T., Martinez Sainz, G., Posetti, J., MacKinnon, R., Hickok, E., Bar, A., Lim, H., Lim, M. 2015, *World Trends in Freedom of Expression and Media Development: Special Digital Focus 2015*, UNESCO Publishing, Paris 46 <<http://unesdoc.unesco.org/images/0023/002349/234933e.pdf>>.

including ethical policies. Technology provides some useful solutions to supporting limited human resources. We believe that "responsible AI" will play a key role in this regard in future. Ethics matters.²¹ The defence of ethical values embedded into computer systems, Multi-Agent Systems (MAS) and AI is a hot topic now, bringing together (i) *thoroughness* (the sound implementation of what the system is intended to do), (ii) *mindfulness* (those aspects that affect the individual users, and stakeholders) and (iii) *responsibility* (the values that affect others).²²

A range of industry terms are used to refer to measures that are built into systems while they are being developed. A generally-used term is "Compliance by Design" (CbD) which is often used to refer to compliance control measures with a limited scope, for example permission-based access controls and alert generation to support compliance monitoring. For enhanced compliance design measures that enable the automated management of the complex governance, management, technical and legal domains, the term "Compliance through Design" (CtD) is used. Both entail the embedding of requirements of each of these domains into an overall business, management or administrative process during the design phase, with CtD being able to manage more complex legal processes.²³

Currently, controls for facilitating complex legal and governance compliance can only be partially automated.²⁴ CbD solutions can however be successfully applied to support human compliance decisions. As technology develops basic CbD could be enhanced to CtD to enable increased automation of basic human authorisation and control processes. CtD expands and improves the use of technical languages to manage rights and duties through algorithmic governance, web services, and semantic web approaches (mainly ontologies).²⁵

The Commission is urged to consider the use of the compliance technologies to facilitate compliant and transparent government action, especially where decisions and actions may impact on human rights. Specific thought should be given to the role of the Commission in a three-pronged approach

²¹ P. Casanovas, 2015. Semantic web regulatory models: Why ethics matter. *Philosophy & Technology*, 28(1), pp.33-55

²² Noriega, P., Verhagen, H., d'Inverno, M. and Padget, J. (2016). A manifesto for conscientious design of hybrid online social systems. In *Coordination, Organizations, Institutions, and Norms in Agent Systems XII*, Springer, Cham, pp. 60-78.

²³ P. Casanovas, J. González-Conejero, L. De Koker, "Legal Compliance by Design (LCbD) and through Design (LCtD): Preliminary Survey", Proceedings of the 1st Workshop on Technologies for Regulatory Compliance co-located with the 30th International Conference on Legal Knowledge and Information Systems (JURIX 2017), Luxembourg, December 13, 2017, pp. 33-49 CEUR-2049 <http://ceur-ws.org/Vol-2049/05paper.pdf>

²⁴ This was one of the conclusions of the VIRTUOSO Project (Versatile InfoRmation Toolkit for end-Users oriented Open Sources exploItation) http://cordis.europa.eu/result/rcn/164431_en.html Cfr. Koops, B.J. and Leenes, R., 2014. Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology*, 28(2), pp.159-171.

²⁵ Casanovas, P., Irujo, J.A., Melero, F., González-Conejero, J., Molcho, G. and Cuadros, M., 2014, November. "Fighting Organized Crime Through Open Source Intelligence: Regulatory Strategies of the CAPER Project". In *JURIX*, Amsterdam: IOS Press, 189-198.

to increase public and private investment in responsible, ethical AI, preparing for socio-economic changes, and to developing an appropriate ethical and legal framework (researchers, laboratories and start-ups).²⁶

5 Governance and management of technology

The usage of technology may hold positive or negative impacts on human rights depending on factors such as the type of technology employed, the context in which it is employed and the governance and management of its usage.

Technology, and more specifically AI, can be used to protect personal data, create secure environments, promote innovation, ensure citizens' participation, reinforce collective identity, and facilitate legal and administrative organisation both in private and public spheres. We call the overall approach *linked democracy*, a step ahead of deliberative democracy, i.e. a smart way to organise knowledge, institutions, and people through responsive and responsible regulations.²⁷

The impact of the use of enhanced data technologies in Australia will however greatly depend on a range of human and governance factors, including:

- The ability to correctly and fairly identify and assess the risks and benefits of a particular solution in relation to the state, society and individuals and the likely effects of its usage on them, prior to its implementation as well as continuously, after implementation.
- The ability of those who manage the technology and those who are accountable for it, to make appropriate, informed and fair decisions and to convince the public to trust the quality and integrity of those decisions.

In some cases, especially where public trust is vital, it may require a degree of transparency or translucency of the technology used.²⁸ In general however, it will require significant investment in public education and in developing the skills of senior public officials and corporate officers who are charged with the management of governance of such technologies. In certain cases it would also be appropriate to ensure that decision-takers have the benefit of independent technological advice to

²⁶ See Brussels, 25 April 2018, http://europa.eu/rapid/press-release_IP-18-3362_en.htm , <https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe>

²⁷ See M. Poblet, P. Casanovas, V. Rodríguez-Doncel, *Linked Democracy*, cham: Springer Briefs, 2018 (forthcoming).

²⁸ Bennett Moses L and de Koker L, 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data for National Security and Law Enforcement Agencies' (2017) 41(2) *Melbourne University Law Review* 530 <<http://classic.austlii.edu.au/au/journals/MelbULawRw/2017/32.html>>.

ensure that their decisions are informed and consistent with Australia's international human rights obligations.

6 Internet access as a human right?

None of the international human rights instruments confer an express right of access to the internet on individuals. A number of commentators have argued, however, that internet access has become vital to the ability of individuals to participate in and enjoy the benefits of substantive human rights such as the right to freedom of expression as well as ESC rights such as the right to development, health and education.

Commentators have also noted that the absence of access to the internet has the tendency to create a 'digital divide' where those without access become increasingly marginalised and locked out of the economic and social benefits provided by the internet and internet-based services.

Digital divides also have the effect of increasing the vulnerability of marginalised populations to closed internet-based environments provided by Big Tech. For example, in Indonesia and other south east-Asian countries, it is claimed that 'Facebook is the internet.'²⁹ The result is that populations in developing countries may have their access to the internet mediated through single service providers.

In our submission, limited or mediated internet access excludes and marginalises individuals from services that are vital to realising human rights. However, as the AHRC's role in addressing these issues is limited under its current authorising legislation it will be important for it to carefully consider how it can best advance a human rights approach to internet access issues.

7 Information security as a human right

Online information security (cyber security) is one of the most intractable issues of the information age. Serious cyber security breaches have become a daily event and, despite the efforts of the national public and private sectors and international initiatives designed to address, prevent and mitigate cyber security risks, the cyber security environment is deteriorating.

²⁹ See <https://www.smh.com.au/world/asia/facebook-is-the-internet-for-many-people-in-south-east-asia-20180322-p4z5nu.html>

Article 3 of the Universal Declaration of Human Rights (Declaration) confers on individuals ‘the right to life, liberty and *security* of person.’ Although there is debate about the nature and extent of the right to security, a significant body of opinion considers that this right can extend to individual security in the online environment. The Declaration and the *International Covenant on Civil and Political Rights* (ICCPR) also confer cognate rights to privacy.³⁰ Privacy rights in online activities necessarily involve the security of personal information collected, used and disclosed through accessing and using internet-based services.

Noting that the AHRC has no existing legal authority to undertake cyber security regulatory activities, the threshold issue for it is to determine a position on cyber security as a human right. If it comes to the view that cyber security is a human right, it will be required to determine how best to go about addressing these issues and to establish its roles and responsibilities. Should it seek to embody cyber security rights within Australian law? If so, how should these be defined and how should they be conferred? Short of this, what functions does the AHRC have in the current debates about cyber security?

8 Privacy

Australia has the weakest legal protections for privacy of any of the members of the OECD. There is no human right to privacy. There is no statutory tort of privacy infringement and common law privacy protection is, at best, uncertain.

Online services harvest personal information for commercial purposes – primarily to sell information to enable advertising that is micro-targeted at individuals. Big Data techniques³¹ enable personal information to be processed to produce insights into individuals and to analyse their characteristics and behaviours in ways that can be highly intrusive. Big Data presages AI as AI is based on the availability of large amounts data, high speed computer processing and algorithmic decision-making.

Although the phenomenon of Big Data gives rise to privacy concerns, it also engages other human rights issues such as discrimination. As is recognised in the Issues Paper there are numerous examples of algorithmic decision-making in areas as diverse as credit scoring, determining an individuals’ sexual orientation and preferences, recidivism and liability to repay social security

³⁰ Article 12 of the Declaration and Article 17 of the ICCPR.

³¹ Casanovas Romeu P, de Koker L, Mendelson D and Watts D “Regulation of big data: perspectives on strategy, policy, law, and privacy” 2017 *Health and Technology* 335-349.

benefits that result from opaque, black box decision-making processes³² that are unknown to the individuals concerned and which have discriminated against minorities or the vulnerable.

The AHRC has a responsibility to address these issues by considering the regulatory measures that should be put in place to protect individual human rights to privacy in an era of Big Data and the developing era of AI.

Thank you for the opportunity to comment on the Issues Paper. We would be happy to further engage with the Commission as its work in this area develops.

Yours sincerely,

Professor Pompeu Casanovas

Professor Louis de Koker

Dr Andre Oboler

Ms Mira Stammers

Professor Anne Wallace

Professor David Watts

On behalf of La Trobe LawTech



La Trobe LawTech

³² Bennett Moses L and de Koker L, 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data for National Security and Law Enforcement Agencies' (2017) 41(2) *Melbourne University Law Review* 530 <<http://classic.austlii.edu.au/au/journals/MelbULawRw/2017/32.html>>.

The La Trobe LawTech team

- **Professor Pompeu Casanovas**, the founding director of the Autonomous University of Barcelona's Institute of Law and Technology. Pompeu has more than 30 years' experience conducting research on legal sociology, pragmatics and artificial intelligence.
- **Professor David Watts**, the Professor of Information Law and Policy at the La Trobe Law School. David is the Big Data lead for the UN Special Rapporteur on Privacy and a member of the UN's data privacy advisory group, Global Pulse. He is the former Privacy and Data Protection Commissioner for the State of Victoria.
- **Professor Louis de Koker**, the Program Lead: Law and Policy at the Data to Decisions Cooperative Research Centre. This program combines the research strengths of La Trobe Law School, Deakin Law School and UNSW Law.
- **Professor Patrick Keyzer (FAAL)**, Head of La Trobe Law School and the Chair of Law and Public Policy at La Trobe. Patrick's recent work has analysed the impact of social media on the relationship between the courts and the law, and the implications of AI and the law.
- **Professor Anne Wallace**, the Associate Head of La Trobe Law School. Anne studies the development, implementation and impact of information and communications technology on court processes.
- **Professor Jianfu Chen**, who specialises in international and comparative law, Chinese law, international business and trade law, globalisation and law, and human rights law.
- **Professor Nicholas Morris**, an adjunct professor at the La Trobe Law School, a visiting fellow at the Martin School, Oxford, and a guest professor at the China Executive Leadership Academy, Shanghai. Nicholas has been Deputy Director of the UK Institute for Fiscal Studies and led various economic consultancies including London Economics.
- **Associate Professor Sara M. Smyth**, is the Director of La Trobe's Master of Laws program and the Coordinator for the Masters of Cybersecurity Program (Law). Sara consulted extensively to Public Safety Canada and has written several books, including *Drone Controversies – Ethical and Legal Debates Surrounding Targeted Strikes and Electronic Surveillance* (2016).
- **Dr Andre Oboler**, the founder of the Online Hate Prevention Institute, is recognised as a leading international expert in the regulation of online content. Andre serves on the Australian Government's delegation to the International Holocaust Remembrance Alliance and on the IEEE's Global Public Policy Committee.

Mira Stammers is a lawyer, NewLaw entrepreneur, academic and author. A pioneer in legal innovation, Mira is the founder of legallyours.com.au, one of the first online legal marketplaces in the world. Mira researches and teaches Legal Disruption at La Trobe University.