WESTERN SYDNEY
UNIVERSITY

Attention: Project Team
Human Rights and Technology Project
Australian Human Rights Commission

Dear Project Team

RE: SECOND STAGE CONSULTATION ON HUMAN RIGHTS AND TECHNOLOGY DISCUSSION PAPER

Overview

1. Information is power in our modern world. As technology ramps up efficiencies and more and more data is able to be amalgamated, sorted, and tracked, those with ownership and access to data are also the owners of immense power. Whenever there is an imbalance of power the law needs to be forward thinking and adaptable to protect fundamental human rights. Researchers at our institution commend the Australian Human Rights Commission for highlighting the urgency of reform as technology outpaces our existing regulatory frameworks.

2. As a group of academics working at Western Sydney University, human rights protection is at the forefront of our concerns. Known as the law degree 'with a social conscience' we have a commitment to our community through developing research that is informed by ethics and notions of justice. While the intersection between human rights and the regulation of technology has been relatively recent, it is a growing field of enquiry. At Western Sydney University we are concerned that concepts of human rights infuse our curriculum, including in our more recently introduced courses Technology, Innovation and the Law and Designing Law Apps for Access to Justice. It is our duty as lawyers and researchers to make sure human rights are protected in policy and legislation, and with the advancement of technology predominantly in a private, unregulated, or self-regulated space, the ability for human rights abuses is constantly growing.

3. This submission supports a number of the proposals put forward by the Discussion paper. Our contribution to this discussion, apart from lending support to those arguments already adequately debated and expressed, is primarily to highlight a

significant problem with the current state of regulation in this space and add our voices to strengthen the call for reform.

4. The specific proposals we wish to comment on are:

    1. Proposal 1
    2. Proposal 2, Question 'A'
    3. Proposal 4
    4. Proposals 5-10
    5. Proposal 11
    6. Proposal 15
    7. Proposal 29

Support and critique for Specific Recommendations

Proposal 1- adopt the FinTech model and an educational approach

1. Proposal 1 (c) involves the promotion of effective regulation – including law, co-regulation and self-regulation. We would recommend adopting a similar approach and model to the one that has existed for FinTech start-ups involving an effective regulation due to the mix of regulatory approaches. For example, the FinTech community enjoy the benefits of ASIC's Innovation Hub[1] engaging and supporting Industry, ASIC's hosting of Industry Liaison's, offering community engagement, sandbox regulation and exemptions for specific FinTech's. This approach should be adopted when examining AI technology designing specifically for vulnerable

[1] Australian Securities and Investments Commission, *Innovation Hub* (Web page) <https://asic.gov.au/for-business/innovation-hub/>

populations so that a more rigorous consultation can occur, and the burden does not fall on the small number of existing providers creating AI technology solutions for vulnerable populations, specifically with disability in mind.

2. In response to Proposal 1(d) – we advocate adopting an educational approach similar to that of The Inclusive Design Research Centre at OCAD University[2] whereby the international community of open source developers, designers, researchers, advocates and volunteers work together to ensure that emerging information technology and practices are designed inclusively.

Proposal 2- clarify the term 'AI'

1. Proposals 1 and 2 incorporate the prioritising and establishment of inquiries over ethical frameworks and human rights protection in emerging technologies. Both the independent body proposed in proposal 2 and the Commission proposed in Proposal 3 are more narrowly targeted to 'AI regulation." That means a definition of AI needs to be adopted that is easily adaptable around new technologies and not overly proscriptive. The question is asked whether the Commission's definition of 'AI-informed decision making' is appropriate for the purposes of regulation to protect human rights and other key goals? The current definition proposed has the following two elements: "there must be a decision that has a legal, or similarly significant, effect for an individual; and AI must have materially assisted in the process of making the decision." However, in this context, what would count as 'AI'? While the Discussion paper notes that it is a term of imprecision it continues to use it when referring to regulation. If legislation were to adopt the term this could be problematic, and we would argue that now is the best time to clarify the definition in a manner that is more readily understood.

2. AI is a broad discipline containing diverse subfields and is linked to cognitive behaviours and the philosophy of the mind. Professor John McCarthy who coined the term 'Artificial Intelligence" in 1965 defines AI as the "science and engineering of making intelligent machines, especially intelligent computer programs". The Society for the Study of Artificial Intelligence and Simulation of Behaviour states that AI is

[2] The Ontario College of Art and Design University, *Inclusive Design Research Centre* (Web page) <https://idrc.ocadu.ca/about-the-idrc>

about giving computers behaviours which would be thought intelligent in human beings."[3]

The term 'AI', 'big data', and 'machine learning' are often used interchangeability although there are subtle differences between the concepts. The Gartner IT glossary provides a popular definition of 'big data' to mean '… 'high-volume, high-velocity and high- variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.'[4] Big data is also described in terms of the 'three Vs' where volume relates to massive data sets, velocity relates to real-time data, and variety relates to different sources of data. However, according to Rob Kitchin and Gavin McArdel, there are a number of multiple forms of big data and not all share the same traits.[5]

Machine learning can be separated into supervised algorithms that are developed based on labelled data sets i.e. algorithms can be trained on how to map input and output data while unsupervised learning is where algorithms are left to find irregularities in input data without any instructions as to what to look for.

AI can be seen as a key to unlocking the value of big data and machine learning is a technical mechanism that underpins and facilitates AI. The combination of AI, Big data and machine learning can be called 'big data analytics.'[6]

Therefore, the proposed definition of AI by the Commission does not capture the three concepts of adequately. Further clarification of the term is required.

[3] The Society for the Study of Artificial Intelligence and Simulation of Behaviour, *What is Artificial Intelligence*, (Web page) <https://aisb.org.uk/latest-news/>
[4] Gartner IT, *Gllossary 'Big Data'* (Web page)< https://www.gartner.com/en/information-technology/glossary/big-data>
[5] Rob Kitchin and Gavin McArdel, 'What makes big data, big data? Exploring the ontological characteristics of 26 datasets,' (2016) 3(1) *Big Data Society* <https://journals.sagepub.com/doi/10.1177/2053951716631130>
[6] See UK Information Commissioner's Office, 'Big data artificial intelligence, machine learning and data protection', Version 2.2, at 8. <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>

Proposal 4- strengthen efforts to recommend Government introduce a statutory Privacy tort or push for a Federal Human Rights Act

3. Proposal 4 asks whether the Australian Government should introduce a statutory cause of action for serious invasions of privacy. While a difficult concept to define, privacy has long been accepted as a human right, and plays a significant role in the relationship between citizens and their governments. Both Article 12 of the *Universal Declaration of Human Rights* and Article 17 of the *International Covenant on Civil and Political Rights* require signatory states to implement basic data protection principles, including the right to ascertain what personal information is stored in data cachets and for what purposes. The implementation of a statutory tort is a long standing call for reform borne out of the fact that the courts are yet to take up the invitation from the High Court in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* to develop one through the common law.[7] The decision in *Glencore*[8] and the ACCC's report on the Digital Platform's Inquiry[9] raise the similar concern on the absence of such a tort. It would also bring Australia into a comparable position along with other common law jurisdictions.[10]

   Significant gaps exist in the way information privacy is regulated at the moment. While the Australian Privacy Principles (APPs)[11] mandate certain requirements, there is nothing for a citizen to do but complain after a data breach has occurred, and therefore, cannot be undone. There needs to be further recognition that a data breach involving personal information can put affected individuals at risk of serious harm. The *Notifiable Data Breaches Scheme* can barely hold a feather to the pro-citizen approach the *General Data Protection Regulation* provides in Europe. In

[7] (2001) 208 CLR 199.
[8] *Glencore International AG v Commissioner of Taxation* [2019] HCA 26. In this case legal professional privilege was only available as a shield rather than a sword i.e. was not a freestanding cause of action.
[9] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Web page) <https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry>
[10] Canada has a statutory tort for invasion of privacy and the UK has enlarged their equitable action for breach of confidence as a result of the case of *Campbell v MGN Ltd* [2004] 2 AC 457 and the introduction of their *Human Rights Act 1998*. Protection from breach of privacy in the form of disclosure of private facts has been developed as an independent tort in New Zealand: *Hosking v Runting* [2005] 1 NZLR 1. In America there is also an independent tort of invasion of privacy: it involves the unreasonable intrusion on solitude, public disclosure of private facts, publicity which presents the plaintiff in a false light and appropriation of the plaintiff's name or visage.
[11] Schedule 1 *Privacy Act 1988* (Cth).

particular the exemption for individuals, political parties and small businesses does not meet the minimum requirements under the GDPR.

The *Notifiable Data Breaches Scheme* requires companies that come under the *Privacy Act*[12] to voluntarily notify people when sensitive data has been breached, either for malicious or criminal attacks, human error, or system defaults. The results of these breach reports are alarming[13], perhaps showing why the uptake on the My Health Record system was so low.[14] Nevertheless, where does this leave the individual? How can the data breach be unmade? The breaches scheme allows the Information Commissioner to investigate but as with breaching the personal privacy, to have the orders enforced requires re-litigation in the Federal Courts.[15] Is the *Privacy Act* enough of a deterrent to make sure companies not only have plans in place for data breaches but also are using information appropriately?

Gaps in the *Privacy Act* are also numerous. Once data becomes de-identified the APP's no longer apply, yet for a lot of data, there can be ways to 're-identify' the data. This was proven when a Melbourne University researcher was able through Freedom of Information applications to collect and re-identify Medicare data.[16] The *Privacy Act* also does not extend to media organisations or to private persons.[17] The Information Commissioner is able to investigate breaches of the APPs and even in some instances declare compensation. Those orders, to be enforceable, need to be re-litigated in the Federal Court which can be costly and time consuming. Recent Commissioner decisions also highlight how hard it can be to draw the balance between an individual's privacy and the government's power over their data. An example of this is where a Minister provided a citizen's tax returns to the media to retort to criticism which was then upheld by the Information Commissioner.[18]

---

[12] Namely Government organisations and private sector organisations with a turnover of over $3 million- *Privacy Act 1988* (Cth) S6C.
[13] OAIC *Notifiable Data Breaches Quarterly Statistics Report: July-December 2019*: available at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2019/.
[14] Louisa Walsh, Sophie Hill and Meredith Allan, 'A content analysis of the consumer-facing online information about My Health Record: Implications for increasing knowledge and awareness to facilitate uptake and use' (2018) 47(3) *Health Information Management Journal* 106.
[15] *Privacy Act 1988* (Cth) S55A.
[16] Vanessa Teague, Chris Culhane and Ben Rubinstein, 'The Simple Process of Re-identifying Patients in Public Health Records.' (*The Pursuit*, University of Melbourne, 18 December 2017). https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records.
[17] S7B (4)
[18] Darren O'Donovan, 'Who, What, When, Administering the Media' *The Mandarin*, (online, 26 June 2018) <https://www.themandarin.com.au/94880-who-what-when-administering-the-media/>

Consider the sanctions and fines under the GDPR of up to ten million euro or more as compared to the limited compensation likely to be awarded through the OAIC.

There are other privacy concerns in various areas not covered by information privacy laws. Surveillance through location tracking, facial recognition, drones, and targeted advertising are all areas that are in need of consideration. Ongoing issues continue to exist in relation to regulating revenge porn, [19] stalking, online harassment, and online scams. These issues do not fit neatly into existing statutory schemes. The *Telecommunications Act* and state equivalent surveillance devices Acts were largely written before the development of things such as remotely piloted aircrafts. The piecemeal approach of a patchwork of different laws are always going to leave gaps. A statutory privacy cause of action would help fill in those gaps. Media organisations have long opposed such a recommendation[20] but the inadequacy of our laws will continue to become apparent as new emerging technologies are used and abused.

A statutory cause of action may also help re-dress the social effects of a country that allows citizens to be tracked and recorded. As Foucault warned us in *Discipline and Punish* the ordering gaze can have real effects on how an individual behaves. People who are under surveillance are not able to act like themselves and the pressure to conform can have impacts on a person's psyche. Having an action will allow citizens to re-balance the power structure, if even in a small way, and signify the importance of such a fundamental human right such as privacy.

If the Government remains reluctant to introduce a statutory cause of action, we would recommend that more pressure be exerted into the push for a Federal Human Rights Act similar to that of New Zealand and a number of states.[21]

Recommendation: <u>strongly</u> encourage the Government to introduce a statutory cause of action for serious invasions of privacy. If the government proves reluctant more pressure for a Federal Human Rights Act is needed.

---

[19] Especially considering the relevant *Crimes Act* offences (such as s578C (2)) require publication and the case of *Burrows v Commissioner of Police* [2001] NSWIRComm 333 at [110]-[114] held that sending an image to a single individual does not fall into the definition of 'publish.' While the equitable doctrine of confidentiality may fill in this gap, the courts are notoriously slow at tackling such issues and a statutory intervention is urgently required.

[20] See for e.g. the Standing Committee on Law and Justice 'Remedies for the Serious invasion of privacy in New South Wales' Report of March 2016.

[21] See Justin Gleeson SC, 'A Federal Human Rights Act- What Implications for the States and Territories?' (2010) 33(1) *University of New South Wales Law Journal* 110.

Recommendation: Introduce a rebuttable presumption against the lawfulness of AI-based decision-making that fails to provide people with adequate and clear explanations

Recommendation: Introduction of mandatory transparent data collection

4. Proposals 5 to 10 concern administrative decision making and AI and a number of ways this can be regulated. The regulation of administrative decision making carried out through algorithms and using big data raises a number of issues. There are the issues of protecting privacy, whether commercial secrets and code copyright infringement can interfere with an individual's ability to challenge decision making, the extent of the process of decision making and whether bias in algorithms can be challenged or minimized, as well as who has access to private data and what should be the repercussions for small or big scale data leaks? Proposal 5 is about informing an individual when AI is used, proposal 6 looks to help Government keep human rights in mind when looking at using these type of services, Proposal 7 looks at legislation requiring explanations of how AI decisions are made whereas Proposals 8,9 and 10 are about introducing accountability into these systems.

   Big data analytics technologies and tools that enable big data analytics are becoming increasingly the norm for businesses. It is obvious that governments would want to incorporate more efficient methods as services scale upwards. As this occurs it may be difficult to draw a clear line between big data and more conventional forms of data use. This is because although big data involves personal data that may directly identify individuals, in many instances big data analytics do not involve personal data. For example, non-personal data such as world climate and weather data, geospatial data from GPS equipped busses to predict arrival times, data from sensors on containers carried on ships enable improved services and business processes. Such data do not involve personal data.

   It is not easy to identify if a particular instance of data processing is or is not big data analytics because in some cases it may appear to be simply a continuation of

processing that is the norm. For example, banks and telecommunications companies generally process large volumes of data and credit card issuers have had to validate consumer purchases in real time. Companies may not want to disclose how personal data is processed on the grounds that it is difficult to predict how personal data may be processed based on how the AI algorithms may be used for machine learning. However, it is important to consider the implications of big data analytics for data protection. AI technologies are used for big data analytics, as well as behavioural tracking technologies. AI as a profiling tool is increasingly being used by businesses to enable big data analytics. How can data collectors ensure that consumer data is being processed transparently and not breaching the law and what measures can be imposed to regulate the use of big data analytics technologies and tools?

The implications of making human lives subject to the autonomous computers generating their own solutions are manifold. How do we make accountable a process? If there is no-one but a computer to blame how does a citizen seek redress? While the potential for efficiency gains are huge, so is the potential for human right infringements. The recent case of *Pintarich v Deputy Commissioner of Taxation*[22]has proved that the law is not quite ready to give a computer the title of 'decision-maker' due to the lack of mental process in reaching a decision. As stated in *Semuningus v Minister for Immigration and Multicultural Affairs*,[23] a valid decision requires a mental process of reaching a conclusion. However, where intelligent design is concerned it is likely that a decision can be made by AI technology that uses deep learning neural networks to create solutions.

Freedom of Information access to decision making tools are part of the administrative lawyer's toolbox and a critical step in ensuring lawful decisions are being made. With exceptions surrounding commercial secrets, decisions made by algorithms become problematic. In Spain a situation arose where an electricity subsidy was denied to half a million people due to a software malfunction- however proving the mistake was problematic due to no access to the source code. Even in countries where source code is treated like a document under freedom of information laws, algorithms have still been able to be kept secret.[24]AI and Big Data analytics draw inferences and predictions about people drawn from diverse data that is sometimes hard to predict, understand, or refute. Individuals are granted little control over how this data is then used to make certain inferences about them. Without a human decision maker, the objective and necessity of discretion is also evaporating. Controls for accountability including procedural fairness, dictate that

[22] [2018] FCAFC 79 (Special Leave refused by High Court)
[23] [1999] FCA 422
[24] Nicolas Kayser Bril 'Spain: Legal Fight over an algorithm's code' *Algorithm Watch,* 12 August 2019

individuals have a right to the information from which certain inferences are made about them when it is taken into consideration for a decision.

The decision making technology is already being used in areas which raises concerns for vulnerable populations. AI-informed decisions are being made in relation to the eligibility of social services and disability entitlements. The annual renewal of NDIS plans in particular using a plan manager with AI powered software solutions to assist with calculating the degree eligibility does not consider the barriers to engaging at this level and the heavy burden of annual admin in order to achieve a greater level of financial assistance. A rebuttable presumption may assist people dealing with these issues and the evidentiary burden in any challenge to a decision.

Recommendation 1: Agree with Proposal 7 & 8 and answer to the Question posed: A rebuttable presumption against the lawfulness of AI-based decision-making that fails to provide people with adequate and clear explanations, is required by procedural fairness.

Recommendation 2: Introduction of mandatory transparent data collection will ensure express and explicit consent similar to the GDPR prior to personal data collection, introduction of privacy by design and for privacy by default may ensure transparency in data collection and processing by data collectors.

Proposal 11- introduce a legal moratorium on the use of facial technology in decision making

5. Proposal 11 asks whether the Government should introduce a legal moratorium on the use of facial recognition technology in decision making that has a legal, or similarly significant, effect for individuals, until an appropriate legal framework has been put in place. This legal framework should include robust protections for human rights and should be developed in consultation with expert bodies including the Australian Human Rights Commission and the Office of the Australian Information Commissioner. Automatic facial recognition has given law enforcement agencies enormous power to collect biometric data that can be used for surveillance and tracking ordinary people. Non-consensual harvesting of biometric data is already outlawed under the European General Data Protection Regulation, a trial operation

of automatic facial recognition in London was ended and, in the US, the City of San Francisco has banned the use of facial recognition technologies from being used. In Australia, there is no standard code of conduct or legal requirements for law enforcement agencies and private operators of public spaces on how biometric data such as facial recognition data (that is considered personal data, as it can be used to identify an individual) is to be collected, stored, and used. The law needs to establish clear rights for individuals over the use of facial recognition technologies that may be embedded in CCTV cameras by the public sector and private sector. The public need to know how their facial recognition data may be collected, used and disclosed. There are also issues around accuracy with these technologies which are not being examined. We are falling behind the rest of the world in terms of regulating these tools and we need to put a hold on their use until the protection of people's human rights can be properly built into some form of regulation.

Recommendation: Introduction of a privacy preserved legal face recognition framework and the prohibition unlawful and non-consensual harvesting of biometric data needs to be developed. Technologies such as privacy by design through the use of cryptographic techniques and image processing operations may be an option to protect facial recognition data from being misused to protect human rights.

Proposal 15- establish a regulatory sandbox

6. Proposal 15 is in relation to a regulatory sandbox. The FinTech regulatory sandbox adopted by ASIC is a good example of the effectiveness of such models. Regulatory sandboxes are risk-controlled, time limited testing environments that enable a business to reduce uncertainty and manage regulatory risks during the testing phase of its innovative product or business model. The Australian Government should consider establishing a regulatory sandbox to test AI-informed decision-making systems for compliance with human rights. In particular, the criteria for sandbox participation should insist on criteria addressing how these technologies would address access for persons with disabilities and whether it is likely to interfere with their human rights. This will set the tone and leadership for building and creating more diverse and inclusive AI environments and technologies. The approvals or exemptions that could be created by participation in human rights compatibility testing would need to be appropriate but also incentivising. Tender documents could require participation for example.

Recommendation: A regulatory sandbox should be adopted, and Government's should require participation through all tenders.

Proposal 29- develop digital communication standards for inclusivity and other standards in line with the three principles of inclusive design

7. The Attorney-General of Australia should develop a Digital Communication Technology Standard under section 31 of the *Disability Discrimination Act 1992* (Cth). We agree that in developing this new Standard, the Attorney-General should consult widely, especially with people with disability and the technology sector. We also agree that the government should develop other types of standards. In doing so, the Australian government should further consider the three principles of inclusive design adopted by the Inclusive Design Research Centre in Toronto[25]. These include recognising diversity and uniqueness, Inclusive Process Tools – 'nothing about us without us', and broader beneficial impact. Designers, companies, and government all have a role to play, by designing, investing, and legislating with difference in mind, so that a design process that is inclusive becomes standard practice. There is clear evidence of the financial, economic and social benefits associated with including those that are left out in design.[26]

   New technologies can make the world more inclusive and enhance the lives for people with disability. Barriers to communication are everywhere and looking at these barriers as opportunities will allow technology to give back to the vulnerable populations by starting a design that is inclusive for everyone from the initial design process. The Australian Human Rights Commission receives more complaints in discrimination on the basis of disability than on any other ground. It is more common than race, gender or age discrimination. Although we as a community are capable at designing physical environments to allow access and

[25]Centre for Inclusive Design, *Three Principles of Inclusive Design* (Web page) <http://centreforinclusivedesign.org/inclusive-design/three-principles-of-inclusive-design/>

[26] Centre for Inclusive design, 'The Benefit of Designing for Everyone' (online report, May 2019) <http://centreforinclusivedesign.org/media/1186/inclusive-design-report-digital-160519.pdf>

entry to premises for people with disabilities, it is important we think about how good we are at managing this when the same kind of access refers to an intangible environment online.

Conclusion

1. It would be naïve to believe governments aren't going to wholeheartedly jump into technology processes that deliver efficiencies at scale. It is therefore important, before the sector of administrative government services are completely transformed, that regulations, tools, and standards are put in place that require human rights to be a number one priority in the design of these technologies.
2. We believe adopting an educational approach, clarifying the terminology, extra legal recourse for privacy violations, and the use of rebuttable presumptions to protect a citizen's right to challenge administrative decisions is desperately needed. We agree with a moratorium on facial technology and that inclusivity testing needs to be encouraged in designing new technologies that may be adopted by Governments.
3. Should it be necessary, the writers would welcome the opportunity to expand upon these submissions. These views are the named researcher's own and do not necessarily reflect those of Western Sydney University.

- This response to the consultation paper has been prepared by Dr Sarah Hook. Dr Hook is a researcher and lecturer in media and IP law. Her research looks at legal theory and its intersection with legal contexts such as defamation, copyright, government regulation, regulation of the press, and other impediments to the free exchange of ideas and expression.

The Submission draws on contributions from a number of academics from the Law School at Western Sydney University:

- Dr Thillagavathy Rajaretnam. Dr Rajaretnam is a researcher in information privacy and data security, corporate information

governance, corporate governance law, and regulation. Dr Rajaretnam has numerous publications regarding data and privacy and is an active member with the Asia-Pacific Privacy Scholars Network (APSN)

- Ms Grace Borsellino. Ms Borsellino is a Lecturer and Course Convenor for Corporate Law and Governance, Technology, Innovation and the Law and Designing Apps for Access to Justice units. Ms Borsellino has been an invited international speaker to universities in Taiwan and Hong Kong delivering conference speeches in areas of Corporate Law, Corporate Culture and the Regulation of FinTech, the Digital Economy, and Blockchain related Cryptocurrencies.

- Professor Catherine Renshaw. Professor Renshaw is an expert on international human rights law. She is a Senior Visiting Scholar at the Faculty of Law, University of New South Wales and a Senior Visiting Fellow at the PM Glynn Institute at Australian Catholic University. Professor Renshaw also acts as an advisor to several human rights NGOs in the Asia Pacific region.

- Professor Steven Freeland- Professor Freeland specializes in International Criminal Law, Commercial Aspects of Space Law, Public International Law and Human Rights Law. He was Dean of the School of Law at Western Sydney University from 2017-2019. He is also Visiting Professor at the University of Vienna; Permanent Visiting Professor at the iCourts Centre of Excellence for International Courts, University of Copenhagen; Adjunct Professor at the University of Hong Kong; Member of Faculty at the London Institute of Space Policy and Law; Visiting Professor at Université Toulouse1 Capitole; Adjunct Professor at University of Adelaide; Associate Member at the Centre for Research in Air and Space Law, McGill University; and a former Marie Curie Fellow (2013-2014). He has been an expert assessor for Government Research

Councils in Australia, Canada, The Netherlands, South Africa, Hong Kong, and has taught at Universities in over 20 countries.

- Professor Michael Head- Professor Head is an expert in Administrative law and writes extensively on government control and abuse of power. Professor Head is the author of a number of legal works, including *Administrative Law: Context and Critique* (4th ed, The Federation Press, 2017), *Emergency Powers in Theory and Practice: The Long Shadow of Carl Schmitt* (Ashgate, 2016), *Crimes Against the State: From Treason to Terrorism* (Ashgate, 2011), *Calling Out the Troops* (The Federation Press, 2009) and *Evgeny Pashukanis: A Critical Re-appraisal* (Routledge-Cavendish, 2007). He also publishes regularly in the fields of socialist legal theory and civil liberties.

Academics who have given support and consideration to the recommendations herein include:

- Professor Anna Cody
- Professor Razeen Sappideen
- Associate Professor/Associate Dean (International) Zhiqiang June Wang
- Deputy Dean Mr John Juriansz
- Dr Hadeel Al-Alosi
- Dr Liesel Spencer
- Elen Seymour
- Simon Kozlina
- Jennifer Whelan
- Sandra Noakes