Law Council
OF AUSTRALIA

Human rights and technology

Australian Human Rights Commission

21 April 2020

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2020 Executive as at 1 January 2020 are:

- Ms Pauline Wright, President
- Dr Jacoba Brasch QC, President-elect
- Mr Tass Liveris, Treasurer
- Mr Ross Drinnan, Executive Member
- Mr Greg McIntyre SC, Executive Member
- Ms Caroline Counsel, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council is grateful to the Law Society of New South Wales, the Administrative Law Committee of its Federal Litigation and Dispute Resolution Section, the Privacy Law Committee of its Business Law Section, and its National Human Rights Committee and Business and Human Rights Committee for their assistance with this submission.

Introduction

1. The Law Council welcomes the opportunity to respond to the second phase of the Australian Human Rights Commission's (**AHRC's**) consultation on Human Rights and Technology. This submission is supplementary to the Law Council's earlier submission responding to the first phase of this consultation,[1] and the Law Council continues to refer to the positions outlined.

2. The Law Council's positions on various AHRC proposals contained in the AHRC's *Human Rights and Technology: Discussion Paper* (2019) (**Discussion Paper**) are discussed below.

3. It is worth noting from the outset that this consultation has proved particularly prescient, coinciding with the Covid-19 pandemic of recent months. As the risk of transmitting the virus has necessitated widespread and prolonged social distancing, technology has assumed an even greater presence in the lives of Australians. Corporations, organisations and service providers are all grappling with how to provide remote access to consumers, and the pandemic has highlighted the critical importance of technology in modern communications and social cohesion, making the issue of human rights and technology even more acute.

Response to proposals

Proposal 1: The Australian Government should develop a National Strategy on New and Emerging Technologies

4. The Law Council supports this proposal. It considers that there is a need for greater government oversight of new and emerging technologies at both the state and territory, and federal, levels. It supports appropriately targeted and balanced regulation of uses of new and emerging technologies by both the public and private sectors.

5. In this regard, the Law Council is pleased that the AHRC's proposal for a *National Strategy on New and Emerging Technologies* (**National Strategy**) anticipates 'a multi-faceted regulatory approach – including law, co-regulation and self-regulation – that protects human rights while also fostering technological innovation', in accordance with international human rights instruments, particularly the UN Guiding Principles on Business and Human Rights (**Guiding Principles**).[2] The Guiding Principles provide an authoritative statement on the emerging relationship between a government's duty to protect human rights and the corporate duty to respect human rights. Indeed, this recognition of the corporate responsibility to respect human rights is a unique feature of the Guiding Principles, and particularly relevant to the regulation of emerging technologies.

6. In response to the questions posed at paragraph 3.5(a), the Law Council recommends that the proposal for a National Strategy should consider whether a new legislative framework would assist in promoting the full suite of rights engaged by new and emerging technologies. In this regard, and as the AHRC has identified in response to the initial AHRC Issues Paper, a number of stakeholders identified the

[1] Law Council of Australia, Submission to the Australian Human Rights Commission, *Human Rights and Technology*, 25 October 2018.
[2] Australian Human Rights Commission, *Human Rights and Technology* (Discussion Paper, December 2019) <https://tech.humanrights.gov.au/sites/default/files/2019-12/TechRights_2019_DiscussionPaper.pdf> ('AHRC, *Discussion Paper*') 33.

lack of a federal human rights act as a significant gap in Australia's regulatory and governance framework for human rights protection in relation to new technologies.[3] The Law Council supports further exploration of the impact of this legislative gap and of the mechanisms for addressing it and suggests that such exploration should include expanding the existing legislation for specific rights protections including in the administrative law framework.

7. The Law Council agrees that the AHRC's proposal for development of a National Strategy, which protects and promotes human rights of all people, and especially vulnerable and disadvantaged groups, is critical to building enduring public trust in technology, noting the importance of practical steps for that protection.

8. With respect to public sector agencies, the Law Council notes that properly considered and managed implementations of new and emerging technologies, including advanced data analytics and artificial intelligence (**AI**), have demonstrated capability to reduce the cost of delivering government services. There is also the potential, through new and emerging technologies, to better target services to areas of greatest need and improve citizens' interactions with government agencies.

9. In the private sector, uses of new and emerging technologies present opportunities for a range of benefits, including the potential to develop new products, access new markets, improve the economy, work more efficiently, better target consumer preferences, and deliver safer working environments.

10. While the Law Council wishes to see these benefits realised, it will be important to address the real anxieties over, and legal issues associated with, new uses of data and technology by both the government and private sector.

11. Within the context of the Covid-19 pandemic, for example, the Australian legal profession has acted to transfer more of its operations online, including to enable lawyers to provide legal services to clients remotely. This has not been without challenges, particularly where legal requirements had not previously kept pace with technical capabilities. Consideration is being given to a number of practical issues, including solutions for the witnessing of affidavits, wills and other solemn documents in the circumstances where face-to-face meetings are not possible or desirable. At the same time, courts and tribunals are moving their operations online to ensure that the administration of justice is able to continue as much as possible during Covid-19. It will be important to monitor their progress, particularly with respect to how diverse groups of Australians fare under these online systems of justice, which are likely to offer an important evidence base for the future delivery of these services.

12. The Law Council recognises the range of concerns individuals have over use of such products, which are often fuelled by exogenous factors such as: stakeholder and citizen anxiety over opaque data sharing between diverse government agencies; excessive surveillance; Cambridge Analytica-style inappropriate uses of data; and the shortcomings of privacy and discrimination laws in addressing differential treatment of individuals (whether or not identifiable) in applications of algorithmically assisted decision-making.

13. The Law Council makes these observations mindful of instances in which AI and algorithmically assisted decision-making systems have been implemented in a flawed or ineffective manner, in some cases causing harm to vulnerable people and, in all cases, reinforcing such anxieties. The compliance system used by Centrelink

[3] AHRC, Discussion Paper, 42.

from 2016 to 2019 provided one such example.[4] It is essential that lessons be learned from such examples.

14. The Law Council considers the engagement of all stakeholders, including civil society organisations and individuals, in developing a national strategy will be a critical step to ensuring that digital trust and social licence are nurtured in areas as sensitive as novel applications of data and AI by government and 'big tech' companies.

15. It therefore recommends that the AHRC consider including a recommendation around community consultation and building stakeholder understanding, buy-in and support in its proposal to government for development of a national strategy. By way of positive example, the Law Council notes the New Zealand Government's recent Data Futures Partnership initiative,[5] which empowered dialogue between citizens and interested stakeholders through knowledge building, crafted explanatory materials and white papers, followed by town hall-style consultations. Of course, the development of any national strategy will need to be sensitive to the restrictions and ramifications of the current Covid-19 pandemic.

16. The Law Council also commends the initiatives of the Australian Government's Office of the Interim National Data Commissioner in consulting, through boardroom table-style discussions, with interested individuals and other stakeholders on development of legislation for government data sharing. These consultations enabled interested parties to actively participate in the shaping of broad policy proposals into drafting instructions for specific legislative provisions. The consultations were conducted in a way that built the capacity of interested parties to constructively (both positively and negatively) contribute to that important drafting process. The Law Council understands that the Office of the Interim National Data Commissioner amended a number of drafting proposals in response to suggestions made in these fora.

17. The Law Council notes that it may be difficult, however, to engage individuals on human rights as an abstract topic, even when translated into specific examples of applications of technologies that can be demonstrated to impact commonly understood fundamental rights such as freedom of political communication. It therefore recommends that any engagement with citizens and other individuals includes examples of the various methodologies and processes that government and businesses might use to evaluate any adverse impacts of particular applications of technology.

18. The Law Council notes in this regard that many individuals are now familiar with the process of environmental impact assessments (**EIAs**) and reporting. In particular, this includes how EIAs address abstract and contentious concerns and are iterative, informed, structured, multi-faceted and multi-party. Many individuals understand that impact assessments form a process that must be followed when certain risk thresholds are met, and that they contribute to a report that aids decision-making by presenting various perspectives and, ultimately, conclusions which weigh and mitigate risks against demonstrated benefits.

19. The Law Council recommends that the AHRC consider including examples of already developed processes in its recommendations to government, and that any

[4] See Law Council of Australia, , Submission to the Senate Standing Committee on Community Affairs, *Centrelink's Compliance Program,* 31 October 2019 <https://www.lawcouncil.asn.au/docs/a6d518a0-9306-ea11-9400-005056be13b5/3704%20-%20Centrelink%20compliance%20program.pdf>.
[5] Stats NZ, *Data Futures Partnership:* New Zealand's Data Future (undated).

recommendations promote development of the proposed national strategy with a focus on how rights-affecting applications of technologies are assessed. The Law Council considers that such an approach to the development of a framework would be more effective than simply stating principles and guidelines which may not build public trust or have practical traction in the decision-making processes of government agencies and businesses.

Proposal 2: The Australian Government should commission an appropriate independent body to inquire into ethical frameworks for new and emerging technologies

20. As the AHRC has identified, there are various initiatives currently underway by government, semi-government and private entities, including various health departments, the Australian Government Digital Transformation Agency and Department of Industry, Innovation and Science, on the ethical and regulatory issues that arise in relation to AI.

21. Recent proposals regarding new technology specific to addressing Covid-19 pandemic issues, have also been proposed, some of which have led to concerns about appropriate oversight, including in times of crisis where the actions of government must nevertheless remain proportionate to the circumstances. For example, digital rights advocates have raised concerns about the potential for government overreach, should sufficient safeguards not be adopted, after the Australian Government announced its plans for a new mobile phone app that would trace the movements of Australians in order that the risk of Covid-19 transmission could be carefully monitored as the country comes out of lockdown.[6]

22. The Law Council supports the commission of a single, independent body to inquire into how existing and proposed ethical, rights, and social impact frameworks address (or can be adapted to address) new and emerging technologies, and to collate the findings of these various initiatives.

23. It recommends that any independent body commissioned to conduct such an inquiry convene a multi-disciplinary group that includes project planning and management experts (well experienced in the application of standards, project management methodologies and business planning) as well as privacy, rights, social impact and ethics specialists and lawyers. Such a group would provide a depth of specialist knowledge, which would greatly benefit the development of an ethics framework for new and emerging technology.

24. The Law Council notes that new and emerging technology, including AI, has a global impact and the use of such products is not limited by national borders. Global opportunities require a global solution. International collaboration on appropriate standards should therefore also be encouraged. Various international standards organisations are evaluating global standards for AI. Standards are usually developed through committees of experts and relevant stakeholders. The joint committee of the International Organization for Standardisation (**ISO**) and International Electrotechnical Commission (**IEC**) (Joint Technical Committee 1) for example, can enlist countries to collaborate on international standards.[7]

[6] Andrew Probyn, 'Coronavirus lockdowns could end in months if Australians are willing to have their movements monitored', *ABC News* (online, 15 April 2020) <https://www.abc.net.au/news/2020-04-14/coronavirus-app-government-wants-australians-to-download/12148210>.
[7] ISO, 'ISO/IEC JTC 1 Information Technology' (Website, undated) <https://www.iso.org/isoiec-jtc-1.html>.

25. Given the range of international initiatives, the Law Council considers that, once consensus is reached on an approach in Australia, Australia should take a more active role and partner with like-minded international organisations to develop a shared approach to AI development and the embedding of a high standard of privacy and ethical principles in AI design.

Proposal 3: The Australian Government should engage the Australian Law Reform Commission to conduct an inquiry into the accountability of AI-informed decision making, specifically addressing AI and the principle of legality, rule of law and promotion of Human Rights.

26. The Law Council supports this proposal. However, it notes the time that will be required for the Australian Law Reform Commission (**ALRC**) to properly conduct such an inquiry and the risk, as has happened in other cases,[8] of government not responding to an inquiry once it is completed.

27. Noting the urgent need to address the numerous issues associated with this unregulated nascent area, the Law Council considers that any recommendation to government for such a referral should include guidance as to timing, including in relation to the publication of interim reports and associated government responses.

28. The Law Council believes that there are essential questions to be resolved with respect to the current and future use of AI and administrative law principles, given the fundamental importance of government decision-making to individuals' lives – whether dealing with Medicare, applying for income support, tax decisions, or applying for a passport. While governments have embraced automation with a digital transformation vision, Australians have historically believed that decision-making by government is and should be done by humans. Challenging government decisions is predicated on that belief, and Australia's administrative law institutions are also built on that expectation. There is a mismatch between Australians' beliefs and administrative law, and much of government (and corporate) practice.

29. Administrative law values include the principle that government decisions should be lawful, fair, rational, transparent and efficient. An AI system can breach all these requirements. Development of such systems must take account of programming errors, the limitations of the binary system, and the need for humans when an administrative discretion is involved.

30. Potential difficulties in complying with administrative law principles which may be raised by the use of AI systems include:

    (a) as flagged above, where a statutory discretion is required – for example, whether two particular people are a 'member of a couple' for the purposes of receiving benefits under the *Social Security Act 1991* (Cth). This is a question requiring considerable judgement;

    (b) programming errors, such as:

[8] See, eg, Law Council of Australia, 'One year on, Government fails to respond to ALRC's Indigenous over-incarceration report' (Media Release, 28 March 2019) <https://www.lawcouncil.asn.au/media/media-releases/one-year-on-government-fails-to-respond-to-alrcs-indigenous-over-incarceration-report>.

(i) reliance on algorithmic systems which produce 'if then' results – these do not easily translate complex legislation or transitional provisions, for example particular provisions taking precedence over general ones;

(ii) a system may not be programmed to include relevant provisions from different parts of an Act, or from different Acts, including broader administrative law obligations such as those in privacy or freedom of information legislation. They may also not take into account underlying principles, such as an obligation on agencies to 'use their best endeavours to assist'[9] the Administrative Appeals Tribunal when it is deciding a matter involving their agency;

(iii) difficulties in interpreting key provisions such as 'citizen… of a foreign power'[10] or importing appropriate cultural significance and context to certain terms, such as sexual harassment, family violence or assault;

(iv) failure to take account of common law requirements, including with regard to statutory interpretation; for example, that legislation is presumed not to operate outside Australia, or that the context and intention require that an Act be applied beneficially – or changing case law;

(v) failure to keep up with statutory amendments, especially for legislation which is amended frequently;

(vi) the potential for business rules to fetter a discretionary power. For example, the system may not be designed or able to consider all the relevant facts, such as whether a homelessness allowance should cover people living in a tent in a park;

(c) questions as to who makes a decision when it is wholly or partially made by an automated system (see further discussion below under Proposal 10);

(d) questions whether a decision can be lawful when it does not reflect the intention of the decision-maker;[11]

(e) automated systems may fail to comply with natural justice; for example, a right of prior response if a decision would be adverse to someone's interests;

(f) an automated decision-maker may fail to identify the correct question, including any relevant or irrelevant considerations;

(g) an automated decision-maker may apply the wrong principle of law, noting that the subtlety of legal principles can be difficult to capture in the design of an automated system;

---

[9] See, eg, *Administrative Appeals Tribunal Act* 1975 (Cth) s 33(1AA) on decision-makers to assist the Administrative Appeals Tribunal.

[10] *Australian Constitution* s 44(i).

[11] As in *Pintarich v Deputy Commissioner of Taxation* [2018] FCAFC 79, in which a taxpayer received a computer-generated letter from the ATO ostensibly waiving most of the general interest charge on a tax debt. It was not the authorised officer's intention. The Full Court of the Federal Court found that the machine-generated correspondence could not be relied upon, since there was no related 'mental' decision involved in its being issued, and only the second letter was lawful. However, Kerr J dissented, stating that citizens were entitled to expect that government letters were lawful and to decide otherwise 'turns on its head fundamental principles of administrative law' and was 'productive of uncertainty'.

(h) an automated decision-maker may fail to include necessary preconditions to the exercise of power;

(i) if an AI system fails to require the user or agency to provide all the essential evidence for matters on which the decision-maker must be satisfied, there may be a breach of the 'no evidence' ground;[12]

(j) an inability to explain the outcomes of computation by an automated system may breach requirements for reasons.

31. Ultimately such questions can only be decided definitively by a court. However, agencies should proactively seek to construct their expert systems[13] so that they comply with administrative law standards and produce lawful decisions or outcomes. Compliance with those standards should not be postponed until required by court or tribunal processes.

32. As the AHRC is aware, in its seminal 2004 report, the Administrative Review Council examined issues arising from increasing use of automated systems and devised 27 Best Practice Principles to prevent problems occurring.[14] Relevant principles, which remain essential benchmarks in this area, include:

(a) Principle 1 – Expert systems … would generally be suitable only for decisions involving non-discretionary elements;

(b) Principle 2 – Expert systems should not automate the exercise of discretion;

(c) Principle 9 – Expert systems should comply with administrative law disclosure requirements – in particular, requirements associated with freedom of information and statements of reasons;

(d) Principle 11 – The team designing an expert system should be made up of a combination of people with technical expert systems knowledge and legal and policy experience;

(e) Principle 13 – Agencies should have robust system-testing processes in operation to ensure the initial and continued accuracy and effectiveness of expert systems used in administrative decision making;

(f) Principle 14 – To ensure the continuing accuracy and currency of an expert system and the material it contains, there should be sufficient funding available for a program of periodic maintenance for the system;

(g) Principle 16 – Officers using expert systems should receive continuing training in order to ensure that they understand the relevant legislation and are able to explain a decision to the affected person;

(h) Principle 17 – In the event that the system malfunctions, there should be officers available who have sufficient training to make the decision manually;

[12] The further question is also raised as to how an AI system would assess evidence—especially where qualitative assessment is required—even if it were provided.
[13] See, eg, Administrative Review Council, *Automated Assistance in Administrative Decision Making* (Report No 46, 2004) 5, [2.1].
[14] Ibid.

(i) Principle 18 – A process – for example, robust quality assurance or auditing – should be in operation to ensure that officers are not using informal workarounds to manipulate the result of an expert system;

(j) Principle 22 – Agencies should have the capacity and the will to conduct internal reviews of decisions manually, where appropriate, particularly where review of a matter involving the decision maker's judgement is sought; and

(k) Principle 23 – External review of administrative decisions should be done manually, in accordance with the procedures and practices of the particular tribunal or court conducting the review.

33. The Law Council suggests that an ALRC review could include the extent to which these principles are reflected in practice at the federal level.

34. There are undoubted benefits from use of automated systems (eg financial benefits, more consistent decisions, less bias, requirements to consider all criteria, release of staff for other functions). However, they must be programmed and operated with attention to administrative law standards. That is an ongoing and demanding task but it is essential if these the advantages are to be fully realised. As the above principles make clear, this involves care in the design stage of automated systems, rigorous pilot testing, ensuring staff understand their electronic platforms, including their limitations, and that there is available adequate technical support for users.

Proposal 4: The Australian Government should introduce a statutory cause of action for serious invasion of privacy.

35. As discussed in the Law Council's recent submission to the Australian Competition and Consumer Commission (**ACCC**) regarding its Digital Platforms Inquiry,[15] for some years, there have been differing views among the Law Council's constituent bodies and expert committees regarding the creation of a cause of action for serious invasion of privacy. In the Law Council's submission to the Department of the Prime Minister and Cabinet's inquiry into a *Commonwealth Statutory Cause of Action for Serious Invasion of Privacy*, it noted that the Law Institute of Victoria, the NSW Bar Association, the Law Society of South Australia and the South Australian Bar Association were in favour of a statutory cause of action. The bodies opposing a statutory cause of action included the Law Council's Media and Communications Committee of the Law Council's Business Law Section (**the Media and Communications Committee**) and the Privacy Law Committee.[16] The Law Society of New South Wales (**LS NSW**) has also previously expressed support for a statutory tort of serious invasions of privacy.[17] Its continued support in the current inquiry context is outlined below.

36. The Law Council's Media and Communications Committee provided a submission to the ALRC's inquiry into *Serious Invasions of Privacy in the Digital Age*. It stated that, in relation to invasions of privacy by the media, 'existing avenues of redress, available through the Privacy Act and co-regulatory media and broadcasting codes

[15] Law Council of Australia, Submission to the Australian Competition and Consumer Commission, *Digital Platforms Inquiry - Preliminary Report,* 15 February 2019, 13-15.
[16] Law Council of Australia, Submission to the Department of the Prime Minister and Cabinet, *A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy*,18 November 2011, 3, [4].
[17] Law Society of NSW, Submission No 122 to the Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*,12 May 2014 <https://www.alrc.gov.au/sites/default/files/subs/122._org_the_law_society_of_nsw.pdf>.

of practice, afford prompt, practical and affordable redress for individuals*'*.[18] In that context, the Law Council noted that, if a statutory cause of action were to be enacted, it would need to ensure there is no chilling effect upon freedom of the media and it should be stated as a right of privacy within the Privacy Act.[19]

37. The Law Council provided a submission to the Senate Legal and Constitutional Affairs Reference Committee's *Inquiry into the Phenomenon Colloquially Referred to as 'Revenge Porn'*. It questioned the necessity of the creation of the cause of action as victims of revenge porn may, in some cases, seek remedies in equity for breach of confidence.[20] The Law Council noted in this submission that the Law Society of South Australia and the South Australian Bar Association supported giving consideration to the creation of a statutory cause of action.[21]

38. In the ACCC inquiry, the Privacy Law Committee continued to oppose a statutory cause of action, although the Privacy and Data Law Committee of the LS NSW supported it in principle.

39. In the current AHRC inquiry context, the LS NSW supports the AHRC's recommendation for a statutory cause of action for serious invasion of privacy, on the basis of the following:

    (a) It considers that laws protecting individuals against breach of privacy have not kept pace with technological developments. New technologies, such as those that enable corporations and governments to establish detailed profiles of individuals based on their personal data and browsing history, present an unprecedented scope for serious invasions of privacy.

    (b) The right to privacy is recognised as a fundamental human right in the *Universal Declaration of Human Rights*,[22] the *International Covenant on Civil and Political Rights*[23] (**ICCPR**), the *Convention on the Rights of the Child*[24] (**CRC**) and other instruments and treaties. Australia's obligations under the ICCPR and CRC – which Australia ratified in 1980 and 1990 respectively – require enhanced protections against breach of privacy,[25] to protect against incursions of privacy enabled by new technologies.

    (c) In particular, and in line with the ALRC's recommendation from 2014, the LS NSW considers that a new tort should cover two types of invasion of privacy: intrusion upon seclusion; and misuse of private information.[26] As the ALRC has recommended, the design of legal privacy protection should be 'sufficiently flexible to adapt to rapidly changing technologies and capabilities, without needing constant amendments'.[27] This recommendation is particularly

[18] Law Council of Australia, Submission to the Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*,14 May 2014, 1.
[19] Ibid 2-3.
[20] Law Council of Australia, Submission to the Legal and Constitutional Affairs Reference Committee, *Inquiry into the Phenomenon Colloquially Referred to as 'Revenge Porn'*,13 January 2016, 4, [21]-[22].
[21] Ibid, [20].
[22] *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948).
[23] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).
[24] *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990).
[25] ICCPR art 17(1), CRC art 16(1).
[26] ALRC, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014), 9.
[27] Ibid, 36.

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.

(d) The LS NSW would also support such legislation at the state level.

40. In addition to a statutory cause of action for serious invasion of privacy, there is the broader question of recognising that privacy should be considered a fundamental right in Australia. In this context, the Law Council supports a federal human rights charter, which would advance a national approach in which human rights are universal, indivisible and interdependent and interrelated, and invite attention to the important obligations of protection.[28] It is currently updating its specific policy on a federal human rights charter which it hopes to release later this year.

41. The Law Council anticipates that privacy would be one of the core rights protected under such a charter.[29] The General Data Protection Regulation[30] (**GDPR**) gives guidance on how this might be approached in a balanced manner in practice. It sets out a range of interconnected rights for 'data subjects' and responsibilities and obligations for 'controllers' and 'processors' – a framework that is designed to protect the interests and privacy of individuals, whilst allowing for the free flow of information that is by necessity required to support the various AI-enabled processes of organisations.

Proposal 5: The Australian Government should introduce legislation to require that an individual is informed where AI is materially used in a decision that has a legal, or similarly significant, effect on the individual's rights

42. The Law Council supports this proposal for the reasons the AHRC has articulated.

43. This proposal is potentially onerous. That does not detract from its value. Meeting that proposal, in order to satisfy the equality principle, requires investment in means of advising individuals materially affected and who are not computer literate, as to how to respond to the invitation, and educating them about how to apply online or alternative avenues which they can use.[31]

44. The cost of providing expert evidence when decisions materially assisted by AI which impact adversely on an individual are challenged in a court or tribunal, as a matter of fairness, should be on the agency/corporation using the AI system.

45. In order to improve the lawfulness of algorithms, legal knowledge should be a necessary component, alongside IT and other areas of expertise, in the composition of teams developing such systems.

46. The Law Council also notes that one of the biggest challenges to protecting privacy in the development or application of AI (broadly defined to include any form of machine automation assisted or enabled decision-making by humans as well as fully

---

[28] Law Council of Australia, Submission to the Australian Human Rights Commission, *Free and Equal: An Australian Conversation on Human Rights* (13 November 2019) 38-41 <https://www.lawcouncil.asn.au/resources/submissions/free-and-equal-an-australian-conversation-on-human-rights>.

[29] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17(1).

[30] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 <https://gdpr-info.eu/>.

[31] See also Proposals 16, 19-21, 23, 26-28; Proposal 6.

autonomous systems) is the use and disclosure of information such as activities, interests or preferences of particular individuals or households (whether or not identifiable) for secondary purposes.

47. Often, personal information about an individual collected for a different primary purpose is able to be re-used in AI to inform how a particular individual or household will be dealt with, in circumstances where because an individual is not identifiable to the operator of the AI system, the secondary use is not a regulated secondary use of personal information about an (identifiable) individual. Data and technology enable decision-makers to use information about particular (but not identified or identifiable) individuals or households and to make decisions about how an individual or household is treated without the affected individual or household knowing that this 'de-identified information' has been collected, used and disclosed in this way, with potential adverse consequences to their rights and interests.

48. Even where an individual is identifiable and the relevant secondary use is therefore regulated under privacy law, issues often arise as to the adequacy of notice and consent and, in particular, whether purported consent is informed, understood, explicit and current.

49. The Law Council recommends that the risks of reliance on notice and consent, and the existing scope of privacy laws in the AI context, should be considered and protections built into any new legislation.

50. It notes that Privacy Impact Assessments, as are used in other contexts,[32] may be a means by which the privacy impacts of AI can be assessed so that strategies for mitigating risks can be developed to ensure that privacy is protected before information is collected and used. These assessments could be expanded to include rights and social impact assessment, although consideration would also need to be given to expanding the range of input and evaluative skills required to properly inform such a broadened and multi-faceted assessment. Safeguards such as data minimisation and purpose limitation should also be implemented to prevent the unauthorised collection, use and disclosure of personal information. Individuals should also be able to seek access to such of their personal information as has been used or generated in the AI system and seek redress if they have been detrimentally affected by a decision made by the AI system.

51. The Law Council notes that, in the European Union, Article 22 of the GDPR[33] contains rules to protect individuals in the context of automated decision-making with a legal or otherwise significant effect on them. The Law Council 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 useful benchmark for how these issues might be approached.

[32] See, eg, Office of the Australian Information Commissioner, 'Guide to undertaking privacy impact assessments' (online, 5 May 2014) <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/>.

[33] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 <https://gdpr-info.eu/>.

Proposal 7: The Australian Government should introduce legislation regarding the explainability of AI-informed decision making.

52. The Law Council supports this proposal. It considers that organisations that use AI should be required to make available to individuals descriptions of an algorithm's functionality where concerns about infringements to their rights arise or where such information is necessary to facilitate achieving natural justice in a decision-making process.

53. Individuals should be able to access an appropriate and reasonable explanation of how algorithms have been used to affect how an organisation (both government agencies and private sector organisations) deals with that individual, including because scrutiny over government decision-making is an indispensable element of liberal democracies. The Law Council considers that the examples provided at pages 84 and 85 of the Discussion Paper illustrate the need for explainability, in order that a decision may be scrutinised for error including statistical or historical bias, and unforeseen consequences, particularly discriminatory impacts on often already vulnerable populations, corrected. While there is a tension between traditional intellectual property rights and transparency or explainability, the Law Council notes that balancing conflicting interests is a process commonly used in existing human rights laws, including existing data protection laws.[34] One possible approach for resolving the tension would be to have two simultaneous avenues for disclosure: the first being public disclosure that is limited in scope, and the second being private disclosure – for example, to a public interest steward – that is detailed in scope.[35]

54. With respect to questions in proposals 7-10 (and 3) on the public law value of transparency, Australia has not yet adopted a similar right to that contained in the GDPR[36] right to legibility. An effective right to legibility would ensure that a person whose personal data has been affected adversely by an automated system is provided with a comprehensive audit trail that can be used for review and audit purposes so that the person can challenge the accuracy of the data.

55. That audit trail needs to be expressed in language which can be understood in ordinary English by persons affected. This is necessary to protect the person's right to privacy and to provide effective reasons. The difficulties are illustrated by *Re Schouten and Secretary, Department of Education, Employment and Workplace Relations,*[37] in which the departmental representative at the hearing said he was unable to explain how the outcome was reached in a youth allowance application because replicating the algorithm used to calculate the 'reduction of actual means' test was no longer possible given the complexity of the database and its programming.

56. Achievement of this goal requires agencies of government to maintain accurate records of the data collected and stored and used by the expert system in its administrative decision-making. There is at present no such requirement. The

---

[34] Stuart Meyer, 'A Looming AI War: Transparency v IP Rights' (Fenwick and West LLP, 25 August 2019) <https://www.jdsupra.com/legalnews/a-looming-ai-war-transparency-v-ip-34524/>.
[35] Ibid.
[36] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1, art 12 <https://gdpr-info.eu/>.
[37] [2011] AATA 365.

recommendation (Proposal 12) for an AI Safety Commissioner and for incentives for compliance with accessibility standards (Proposal 21) would go some way to provide assistance. Legislative changes to right to reasons, now often found in legislation, would also be required.

57. The provision in the *Administrative Appeals Tribunal Act 1975* (Cth) (**AAT Act**) subsection 33(1AA) which imposes an obligation on the person who made the administrative decision to use their 'best endeavours' to assist the Administrative Appeals Tribunal in its decision-making task may be of assistance for those bringing proceedings before the Tribunal. The text could operate as a model for other bodies in the public or private sector which offer dispute resolution.

58. As stated above, databases should also be programmed to provide intelligible reasons.

Proposal 8: Where an AI-informed decision-making system does not produce reasonable explanations for its decision, that system should not be deployed in any context where decisions could infringe the human rights of individuals.

59. The Law Council agrees with this proposition.

60. It further notes that Question B under Proposal 8 asks:

> *Where a person is responsible for an AI-informed decision and the person does not provide a reasonable explanation for that decision, should Australian law impose a rebuttable presumption that the decision was not lawfully made?*

61. There would be no need to provide a rebuttable presumption that the AI aided decision was not lawful. The existing ground of review that, where adequate reasons have not been provided, leading when successful, to an error of law or jurisdictional error should be adequate. However, this suggestion would only be effective where the right to reasons is able to be employed effectively.

Proposal 10: The Australian Government should introduce legislation that creates a rebuttable presumption that the legal person who deploys an AI-informed decision-making system is accountable and legally liable for the use of the system.

62. The Law Council supports this proposal to introduce a legislative rebuttable presumption specifying the legal person who deploys an AI decision-making system as legally liable, but notes that this clarification of liability needs to be accompanied by a clear and cost-effective mechanism for recourse or review of such decisions.

63. It notes that many questions arise as to who makes an administrative decision when AI systems are involved. For example:

    (a) Who makes the decision when it is wholly, or partially made by an automated system?

    (b) Can a decision which by statute is to be made by a nominated individual or delegate be made by a machine? Given that delegates are supposed to act with independence, can an automated system truly be said to exercise

judgment and to operate separately from its programmer or the relevant government agency?

(c) What if the decision contains some aspects made by an individual and the rest by an automated system? Does this mean that an individual would need to challenge numerous individuals as well as the automated system?

64. There are also questions whether a decision can be lawful when it does not reflect the intention of the decision-maker, as in *Pintarich v Deputy Commissioner of Taxation.*[38]

65. To resolve such uncertainty, a solution is to legislate specifically, as has been done by some agencies which use automated systems.[39] In such cases, the legislation states that the agency can use computer programs to make decisions which are deemed to be made by the nominated officer.

66. As set out in Proposal 10, an additional solution is a legislated rebuttable presumption, which, as flagged above, the Law Council also supports.

67. In addition, the Law Council notes that there is a developing trend to mandating human intervention in all cases where an individual might receive a negative decision from an AI-enabled system. For example, GDPR Article 22(3) provides that, in such circumstances, a data subject has 'the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision'.[40]

68. The Law Council does not consider that mandating inclusion of a human-in-the-loop of itself effects a solution: a human may or may not make a sensible and balanced evaluation of machine outputs. It considers that it is sensible to require agencies and businesses deploying AI systems to be accountable for their use of those systems. Such businesses and agencies may (and should) contract with systems suppliers to ensure that appropriate transparency and reliability are built into such systems. Businesses and agencies may (and should) also implement an internal process for evaluating inputs into and outputs of those systems to ensure outputs are only relied on by humans where it is sensible to do so: for example, where the machine will demonstrably and reliably outperform a properly informed human in relation to a particular class of decisions, and there is appropriate review and oversight.

69. The Law Council recommends a clear right of recourse against decisions made relying in whole or materially in part on AI data be available in Australia. It also considers the Australian Government should focus on providing the right of legal entities, including natural persons, to a cost-effective and timely review of decisions made by AI-based systems, including necessary amendments to the *Administrative Decisions (Judicial Review) Act 1977* (Cth) and the AAT Act definition of what is a 'decision'.

---

[38] [2018] FCAFC 79, in which a taxpayer received a computer-generated letter from the ATO ostensibly waiving most of the general interest charge on a tax debt. It was not the authorised officer's intention. The Full Court of the Federal Court found that the machine-generated correspondence could not be relied upon, since there was no related 'mental' decision involved in its being issued, and only the second letter was lawful. However, Kerr J dissented, stating that citizens were entitled to expect that government letters were lawful and to decide otherwise 'turns on its head fundamental principles of administrative law' and was 'productive of uncertainty'.

[39] *Social Security (Administration) Act 1999*, s 6A; *Veterans' Entitlements Act 1986* (Cth) s 4B(1A); *Aged Care Act 1997* (Cth), s 23B.4; *Migration Act 1958* (Cth) ss 495A, 495B; *Road Vehicle Standards Act 2018* (Cth) s 62.

[40] General Data Protection Regulation [2016] OJ L 119/1.

Proposal 11: The Australian 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 AHRC and the Office of the Australian Information Commissioner.

70. The concerns outlined in Chapter 6 of the Discussion Paper in relation to the human rights implications of facial recognition technology are well-founded. As Bruce Schneier, an Adjunct Lecturer at the Harvard Kennedy School has noted, however, facial recognition is 'just one identification technology among many'.[41]

71. The Law Council supports a moratorium on the use of facial recognition technology, but notes that this will have no effect if, in response, governments and organisations deploy other biometric identification technologies instead, such as gait recognition,[42] heartbeat detection,[43] voice recognition or fingerprint scanning. To guard against this possibility, and 'future proof' the AHRC's final report on Human Rights and Technology, the Law Council suggests that any recommendations on this issue refer more broadly to 'biometric identification technologies', rather than only 'facial recognition technology'.

[41] Bruce Schneier, 'We're banning facial recognition. We're missing the point', *The New York Times* (online), 20 January 2020 <https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html>.
[42] Australian Law Reform Commission, *For Your Information: Privacy Law and Practice* (Report 108, May 2008) 406, [9.64].
[43] David Hambling, 'The Pentagon has a laser that can identify people from a distance—by their heartbeat', *MIT Technology Review* (online,27 June 2019) <https://www.technologyreview.com/s/613891/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/>.