The Australian Human Rights Commission
The Human Rights and Technology Project Team
tech@humanrights.gov.au

7 May 2020

Re: Call for submissions — Human Rights and Technology Discussion Paper

Dear Commissioner,

Thank you for this opportunity to provide comments to the Australian Human Rights Commissions' (HRC) inquiry into Human Rights and Emerging Technology. Through our submission, we wish to emphasize the importance of human rights in the digital space and the key role that HRC's report can have on Australian's rights going forward.

Access Now is an international organisation that works to defend and extend the digital rights of users globally.[1] Through representation in 14 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. We engage with an action-focused global community, convene stakeholders through the RightsCon Summit Series, and operate a 24/7 Digital Security Helpline that provides real-time direct technical assistance to at-risk individuals and communities worldwide. As an ECOSOC accredited organisation, Access Now routinely engages with the United Nations in support of our mission to extend and defend human rights in the digital age.

In our submission below, we will focus on responding thematically according to the categories in the white paper, focusing on several of the concrete proposals given their relevance for the advancement of individuals' rights and our expertise on these matters.

[1] More information can be found at: https://www.accessnow.org/

Introduction and framework

We appreciate the approach of proposal 1 and proposal 2 outlined in this section and support the call for a *National Strategy on New and Emerging Technologies* as outlined in **proposal 1**. However, for **proposal 2** we would urge a greater focus on human rights and their application in Australian legislation over the emphasis on ethical frameworks. While the ethics discourse has largely dominated the discussion about the societal implications of AI, human rights have a critical role to play. Ethics may consider broad ethical concepts such as justice, fairness, transparency and accountability which allows for valuable debate about the role of AI in our lives.[2] However, not only are human rights more universal and well-defined than ethics principles, they provide for accountability and redress. In particular the right to privacy alongside a user-centric data protection policy ensures extensive protections for users in this area. In this way, human rights and ethics can be mutually reinforcing.[3]

There is a notable momentum to ensure this focus, as the HRC investigation of these issues comes on the back of the Australian Competition and Consumer Commission (ACCC) final report on Digital Platforms.[4] The ACCC's conclusions on the need for a broad reform of the Privacy Act to better serve consumers is supported by arguments made for several years by academics and interested civil society organizations.[5] The Privacy Act dates back from the pre-internet era and although the original text has been amended and updated over time, it is not fit to protect individuals offline and online. The scope of the law is limited to Australian government agencies across the Commonwealth and states, and private entities with an annual turnover of more than $3 million, as well as some health organisations. This means that a large number of private entities processing data do not have obligations under this law. This lack of harmonised rules has also led to the development of a patchwork of privacy protections for consumers across Australia. In addition, the law gives very little power and rights to individuals; rather it has created a set of boxes to tick for those companies which are regulated by the Act. Most notably, individuals are not empowered to challenge infringements upon their rights, nor are entities required to inform individuals or held responsible for the privacy impacts of breaches which resulted in personal data being compromised.

Need for a Stronger Privacy Act

The recommendations put forward by the ACCC in order to strengthen the Privacy Act — from updating definitions, to refining consent requirements and introducing redress mechanisms — would bring Australia closer to current global best practices and would

[2] Bendert Zevenbergen, "Marrying Ethics and Human Rights for AI Scrutiny," Considerati, https://www.considerati.com/publications/blog/marrying-ethics-human-rights-ai-scrutiny/ .
[3] See "Human Rights in the Age of Artificial Intelligence" for further discussion of the interplay between ethics and human rights in AI
[4] https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report
[5]https://www.theaustralian.com.au/business/business-spectator/news-story/privacy-act-revisions-little-bark-no-bite/48a60ffc989d27dabfdef60ad281b368

ensure that Australian entities stay in step with their international partners. Protecting privacy and personal data is not only necessary to guarantee the rights of people in Australia but a prerequisite to ensure secure flow of data which are at the center of the global digital economy.

In our 2018 submission to the ACCC's consultation on this matter, we recommended an overhaul of existing privacy rules — both for the government sector and for industry.[6]

That year, we also published a report entitled *Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers* in which we elaborated on our experience with the legislative process of the EU's General Data Protection Regulation (GDPR). One of the key components is the need to create binding data protection principles in the law. We propose eight key "minimum standard" principles derived from existing international standards, in particular the Council of Europe's Convention 108 and the OECD guidelines.[7] The principles are: fairness and lawfulness, purpose limitation, data minimisation, accuracy, retention limitation, individuals' rights, integrity and confidentiality and adequacy. These principles should be the basis of any data protection framework and are present in a large number of data protection laws around the world, from the EU GDPR, and most data protection laws that are in place in Latin America and Africa.

In our data protection report we further recommend that the following rights are made binding in any future data protection and privacy law in order to protect individual users' rights:

1. **Right to access** enables users to obtain confirmation from services and companies as to whether personal data concerning them have been collected and are being processed. If that is the case, users shall have access to the data, the purpose for the processing, by whom it was processed, and more.
2. **Right to object** enables users to say "no" to the processing of their personal information, when they have not given their consent to the processing of their data nor signed a contract. This right to object applies to automated decision-making mechanisms, including profiling, as users have the right not to be subjected to the use of these techniques.
3. **Right to erasure** allows users to request the deletion of all personal data related to them when they leave a service or application.
4. **Right to rectification** allows users to request the modification of inaccurate information about them.
5. **Right to information** ensures that users receive clear and understandable information from entities processing their personal data, whether these entities have collected this information directly or received it through third parties. All the information provided to the user shall be provided in concise, intelligible, and easily accessible form, using clear and plain language. This information shall include details about data being processed, the purpose of this processing, and the length of

[6] https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/submissions/submissions
[7] Organisation for Economic Cooperation and Development, September 1980. Guidelines governing the protection of privacy and transborder flows of personal data: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf

storage, if applicable. The entities shall provide their contact details and an email address to allow users to contact them in case there are issues.

6. **Right to explanation** empowers users to obtain information about the logic involved in any automatic personal data processing and the consequences of such processing. This right is crucial to bring accountability and transparency in the use of algorithms to make decisions that impact users' lives.
7. **Right to portability** enables users to move certain personal data they have provided from one platform to another offering similar services. To facilitate this process, interoperability between services shall be encouraged.

Finally, no privacy and data protection framework can be complete without a robust enforcement mechanism which includes an independent supervisory authority (data protection authority — DPA — or commission). Even the best data protection law in the world would be close to meaningless without an authority having the powers and resources to monitor implementation, conduct investigations, and sanction entities in case of data protection violations. Sanctions should be proportionate to the violations and can be in the form of notice to action accompanied with punitive fines. Ultimately, we need human rights bodies with enforceable rights.

Artificial Intelligence

Many human rights issues already exist within the digital rights space, particularly in the use of algorithmic decision making and other statistical systems. However, the ability of AI to identify, classify, and discriminate magnifies the potential for human rights abuses in both scale and scope. This is compounded by the inability to fully explain the outputs of an AI system because they are often too complex for humans to understand. Additionally, the harms facilitated by AI often disproportionately impact marginalized populations. The historic marginalization of these groups is reflected in the data used to train AI systems, and can result in outputs that entrench these patterns.

Given problematic legislation such as the Data Sharing and Release Act and the Identity Matching Services Bill, which would enable the national facial recognition system, Australia should act swiftly to deal with near-term human rights harms of AI, as well as prevent the long-term erosion of human rights. Because Australia lacks constitutional protections for human rights, the government should provide robust legal protections and procedural standards that address the risks posed by AI. AI is often used to replace or augment already opaque government decision-making process, and individuals are often unaware AI is being used in ways that impact their lives. This is exacerbated by the fact that many of the human rights risks of AI are not obvious to the layman. Without appropriate action, Parliament and the Australian government are on track to use AI in ways on par with the world's leading surveillance states and that perpetuate historic injustices against indigenous Australians.

We greatly appreciate the suggestion under **proposal 19** to establish an AI Safety Commissioner as an independent statutory officer. We support the structure outlined in the

Discussion Paper to limit the role of the AI Safety Commissioner as a primarily non-regulatory body.[8] We particularly welcome the Commissioner's role to "support the existing regulatory structure, and build the capacity of regulators and others involved in protecting the rights of people who may be affected by the use of AI in various different settings." In the context of our recommendation to set up a data protection authority/commission, that authority would have jurisdiction over complaints and investigations of data protection and privacy implications of the use of AI systems but it would draw from the expertise, policy guidance, and other capacities of the AI Safety Commissioner. The coordination mechanism of the AI Safety Commissioner and other bodies (as also mentioned in the Discussion Paper) needs further clarification.

Proposal 3: Australian Law Reform Commission to conduct an inquiry

We support the several of the proposals laid out in this section, including the inquiry by the Australian Law Reform Commission (ALRC). In considering what reforms or other changes are necessary to protect the principle of legality and the rule of law, and to promote human rights, we would urge the ALRC to examine existing legislation which compounds some of the concerns around the use of AI (as mentioned in the section above).

In December 2019, we contributed a chapter to *Artificial Intelligence for Better or Worse* by Future Leaders, entitled *Artificial Intelligence and Human Rights in Australia*.[9] The following recommendations for AI in Australia are a result of that research and would substantially mitigate the most detrimental potential impacts of AI on Australian society.

1) **Immediately repeal the Data Sharing and Release Act and the Identity Services Bill**. Both bills ignore the high likelihood of human rights violations, and risk institutionalizing mass, unchecked public surveillance if they are passed.

2) **Conduct a comprehensive inquiry into the impacts of AI and automated decision making on indigenous Australians,** with a view to ensuring such technologies are used to benefit, rather than harm, indigenous communities.

3) **Adopt the International Principles on the Application of Human Rights to Communications Surveillance.**[10] The insertion of AI into Australia's unchecked expansion of domestic surveillance is perhaps the single biggest threat to the rights of Australians. Abiding by these principles would check the worst abuses, and enable the government to protect national security without infringing upon human rights.

4) **Update the Privacy Act and Privacy Principles to provide Australians with affirmative rights to privacy and data protection, and address the unique risks posed by AI.** First, without a right to privacy, there is too much gray area that allows

[8]https://www.accessnow.org/cms/assets/uploads/2020/02/European-Human-Rights-Agenda-for-the-Digital-Age-Recommendations-on-Artificial-Intelligence.pdf
[9] http://www.futureleaders.com.au/book_chapters/pdf/Artificial-Intelligence/Solomon_Andersen.pdf#zoom=80
[10] "Necessary and Proportionate Principles."

entities to creep into privacy violations. Second, comprehensive data protection legislation, like the GDPR in the EU, can anticipate and mitigate many of the human rights risks posed by AI. Both personal and non-personal data is fed into AI systems. Therefore, the protection of personal data is a necessary but not sufficient step toward a legal framework to prevent and mitigate human rights risks and violations caused by the development and deployment of AI systems. Particularly helpful provisions include adopting and implementing the data minimisation and purpose limitation principles and establishing clear legal basis for collecting and processing data, including opt-in consent. Access Now has a detailed guide on how to create a data protection framework that respects human rights.[11]

5) **AI and automated solutions for government services should always include meaningful human control and accountability mechanisms.** Due to the sensitive nature of government services, it is inadvisable to migrate them to a fully automated systems, such as the Centrelink expansion from 2016, which has had a detrimental impact on vulnerable groups. As leading experts have pointed out, such developments "breach principles of ethical administration regarding avoidance of oppression of vulnerable and uninformed citizens."[12]

6) **Develop high standards for government use of AI.**[13] AI systems for government often implicate value judgments that are necessarily linked to the political process in free and democratic systems. For this reason, and the ability of government to directly deprive people of their liberty, there should be high standards for public sector use of algorithmic decision making in general. We recommend referring to Access Now's report, *Human Rights in the Age of Artificial Intelligence,* for the specifics.[14] These include:

    a) Adhere to open procurement standards.

    b) Conduct human rights impact assessments.

    c) Establish strong requirements for transparency and explainability.

    d) Establish accountability and procedures for remedy.

[11] See https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf
[12] Christopher Knaus, "Expert attacks Centrelink Robo-debt and the 'moral bankruptcy' that allows it," The Guardian, December 18, 2018, https://www.theguardian.com/australia-news/2018/dec/18/expert-attacks-centrelink-robo-debt-and-moral-bankruptcy-that-allows-it.
[13] The Department of Industry, Innovation and Science released a consultation on the Government's Approach to AI ethics in April 2019. We hope they take our recommendations into account. For more information, see https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/
[14] See https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

Proposal 4: Statutory cause of action for servious invasion of privacy

One of the key components of a functional privacy or data protection regime is the ability for individuals' rights to be enforced and for individuals to seek remedy. Establishing a statutory tort for invasions of privacy would greatly extend individuals' ability to exercise their rights and keep companies accountable. The creation of a tort for serious invasions of privacy was already recommended by the Australian Law Reform Commission in 2014, since then the need for such an avenue has increased as data harvesting practices are skyrocketing in Australia.[15] It was further suggested in the final report of the ACCC's inquiry into Digital Platforms.[16]

Among the most serious risks facing individuals today are the routine over-collection practices of entities and the breaches of personal data that contribute to identity theft, financial fraud, discrimination and other economic and non-economic harms. Individuals should be able to pursue a private right of action that produces meaningful penalties. Statutory damages for violations of privacy obligations should be an essential element of an effective data protection and privacy law in Australia.

As more data is being shared online and off, it is high time to develop mandatory frameworks for data protection and privacy all around the world to prevent or end these behaviours and put individuals back in control of their information. This will also enable the development of privacy-friendly innovation which is currently limited to a small number of companies that have undertaken a long-term engagement approach to protect their individuals instead of basing their business model in monetising individuals' private information.

Proposal 11: Moratorium on facial recognition

Access Now supports the HRC's call for a legal moratorium on the use of facial recognition technology in government decision making. As seen in other jurisdictions, it is further important to distinguish facial recognition that actively surveils and identifies individuals, versus facial recognition that is used passively *ex post* in investigations as they pose different privacy challenges.[17]

[15] The recommendations in that report can be accessed at: https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/recommendations-17/

[16] https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry

[17] https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

AI's capacity to process and analyze multiple data streams in real time has expanded the scope of mass surveillance around the world, particularly through facial recognition systems. Australia is looking to join a number of countries, from China to the United Kingdom, in rolling out national facial recognition systems for public surveillance and law enforcement.[18] Because these systems enable 24/7 monitoring of the general population, they are neither necessary nor proportionate to the goal of public safety or crime prevention, and therefore violate the right to privacy.[19] In the same breath it should be noted that the UK's system has faced continued legal challenge for precisely that reason.[20] The planned Australian system, called "The Capability," would pool identification photos from various State and Federal government sources into one database, which would then be used to compare, via complex algorithms, footage from the growing number of CCTV cameras around the country.[21]

If a national facial recognition system is established, it is highly likely that the Australian police will seek to incorporate it in policing, despite the global concerns around the use of facial recognition in policing and other key government functions. If broadly deployed, facial recognition software within law enforcement raises the risk of unlawful arrest due to error and overreach. Currently, even the most accurate facial recognition systems do not perform as well on darker skinned faces.[22] Given the error rates of current facial recognition technology, these inaccuracies could lead to increased wrongful arrests due to misidentification, exacerbated by the lower accuracy rates for non-white faces.[23] Countries like Scotland have come to question the efficacy and impact of these technologies and have decided not to deploy them in a proactive/preventative manner.[24] There have also been outright bans by local and state governments in the United States, the most famous being San Francisco and Oakland in California, and Somerville Massachusetts.[25] The California Online Privacy Act provides another useful example as it enacted a 3 year moratorium on the use of facial recognition by police.[26]

---

[18] The creation of the system is awaiting Parliament to pass legislation to allow states and the federal government to share identity information. The Identity Matching Services Bill, which lapsed with the dissolution of Parliament on April 11, 2019 but could be taken back up in the future, would do just that. For the current status of this legislation, see https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6031

[19] See "The Necessary and Proportionate Principles," and Privacy International, "Guide to International Law and Surveillance," August 2017, https://privacyinternational.org/sites/default/files/2017-12/Guide%20to%20International%20Law%20and%20Surveillance%20August%202017.pdf.

[20] https://www.lawgazette.co.uk/news/court-of-appeal-to-hear-facial-recognition-technology-challenge/5102241.article

[21] Melissa Locker, "Yep, Australia's sweeping face-recognition system is just as chilling as its name implies," Fast Company, November 7, 2018, https://www.fastcompany.com/90263940/yep-australias-sweeping-face-recognition-system-is-just-as-chilling-as-its-name-implies.

[22] Steve Lohr, "Facial Recognition is Accurate, If You're a White Guy," The New York Times, February 2, 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

[23] Lauren Goode, "Facial recognition software is biased towards white men, researcher finds," the Verge,Feb. 11, 2018, https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error.

[24] https://www.bbc.com/news/uk-scotland-51449166

[25] https://epic.org/state-policy/facialrecognition/

[26] https://www.salingerprivacy.com.au/2020/01/24/facial-recognition/

Australia's national facial recognition system also risks undermining the right to non-discrimination. Because facial recognition is less accurate for darker skinned faces, it misidentifies those faces more often than white faces. When used in a law enforcement or security context, this could result in more indigenous Australians being mistakenly targeted by law enforcement. Though, in turn, this should not serve as an incentive to embark on new mass data harvesting and the creation of more databases which infringe on individual's rights.

Conclusion

We appreciate the opportunity to further comment on the white paper report published by the Human Rights Commission. While there is plenty of well researched and articulated policy in the report to follow, we recommend that the best way to protect users and prevent predatory business practices is through the implementation of comprehensive data protection or privacy regulation, including a right to access, right to portability right to information, right to object, right to rectification, and a right to explanation. This comprehensive regulatory framework should be applicable to all industries, removing the over-reliance on ethical principles and frameworks.

We remain at your disposal for any further inquiries regarding this consultation or our submission.

Thank you,

[redacted], Policy Analyst for Australia and Asia Pacific | [redacted]