Published in *Artificial Intelligence for Better or Worse* in 2019 by Future Leaders (www.futureleaders.com.au)

Artificial intelligence and human rights in Australia

Brett Solomon and Lindsey Andersen

Although artificial intelligence is already mainstream, experts have only recently started looking into the short- and long-term impacts of AI on human rights. Recently in 2018, artificial intelligence was a key topic at RightsCon, a global conference on the future of the internet hosted by Access Now.[1] There we worked with partners to draft and publish the Toronto Declaration on protecting the rights to equality and non-discrimination in machine learning systems.[2] We then released a report in November 2018, *Human Rights in the Age of Artificial Intelligence*,[3] as a preliminary scoping of the intersection of AI and human rights.

Now we apply the framework developed in our report to examine the impacts of AI on human rights in the Australian context. Our analysis builds on our existing work promoting and defending digital rights in Australia.[4] We argue that the greatest human rights risks of AI in Australia stem from the exacerbation of existing digital rights issues; specifically, an ever-expanding domestic surveillance apparatus, and the use of technology to further the marginalisation and targeting of Indigenous Australians, socioeconomically vulnerable groups, and migrants. These risks are compounded by Australia's lack of legal protections for human rights. Human rights violations

facilitated by technologies such as AI often lurk under the surface, and are easily institutionalised in the name of national security, efficiency, and modernisation. Australia's historic approach to human rights protections — reliance on the inherent rights-respecting aspects of its democratic system and a highly politicised Parliament to pass relevant laws — is insufficient, and blind to the realities of the digital age. We conclude with a series of urgent recommendations for the Australian government to prevent and mitigate human rights harms facilitated by AI, both now and in the future.

Why human rights matter in the AI debate

Through the use of AI in algorithmic decision making, surveillance, and the mere fact that AI is built on troves of personal data, AI has created new forms of oppression that often disproportionately impact marginalised groups. A human rights approach can help mitigate such adverse effects, because "the concept of human rights addresses power differentials and provides individuals, and the organizations that represent them, with the language and procedures to contest the actions of more powerful actors, such as states and corporations".[5]

The ethics discourse has largely dominated the discussion about the societal implications of AI. Considering broad ethical concepts such as justice, fairness, transparency and accountability allows for valuable debate about the role of AI in our lives.[6] However, human rights have a critical role to play. Not only are human rights more universal and well defined than ethics principles, but they provide for accountability and redress. In this way, human rights and ethics can be mutually reinforcing.[7]

First, the problem with Australia's approach to human rights

Australia is the only Western democracy without significant constitutional protections for human rights or a national human rights charter. Rather, Australia has an incomplete patchwork of human rights protections found in the Australian Constitution[8] and the constitutions of a few states and territories,[9] common law, statutory law, and the inherent respect for civil liberties built into a democratic system of government.[10]

Because there is no human rights charter, Parliament is primarily responsible for creating federal human rights protections via legislation. It can even intentionally curtail rights via legislation, and the High Court has little power to intervene.[11] Unfortunately, Parliament has done little. There is a startling lack of legal protection in Australia for the majority of internationally recognised human rights. And although Australia has ratified nearly all the major international human rights treaties, it often does not abide by their terms.[12] While Parliament did create numerous anti-discrimination laws and adopt the Rome Statute of the International Criminal Court, it has largely chosen not to enact human rights treaties into domestic law.

The Australian Human Rights Commission, which oversees Australia's compliance with its international human rights obligations, can hear complaints and resolve breaches of federal anti-discrimination law. However, it has no broad legal authority to act as an arbiter of human rights protections. Like the international human rights system from which it stems, its power lies in shaming the government to push for change.[13]

The specific human rights risks of AI in Australia are in many ways a continuation of existing threats to digital rights. The lack of legal human rights protections has enabled the erosion of certain digital rights, most notably the right to privacy. In July 2018, Access Now released a report examining Australia's approach to human rights in the digital age. The report concluded that Australia appears more than willing to undermine human rights as it struggles to adapt to the challenges of the digital era.[14]

Since 9/11, Australia is reported to have expanded its surveillance laws and practices more than any other nation.[15] Many of these powers exceed measures that are necessary and proportionate to the security threats they seek to ameliorate. They include requirements that telecommunications providers retain customer metadata for access by law enforcement and intelligence without a warrant or judicial supervision, laws that facilitate mass surveillance of the Australian public, and most recently, a law that undermines encryption by requiring tech companies to change and adapt their tools and technologies to law enforcements' requests.[16] Indeed, since 2009, Reporters Without Borders has listed Australia as a "country under surveillance", alongside countries such as Egypt, Kazakhstan, India, Russia and Turkey.[17]

Beyond its internal practices, Australia plays an important international role in the respect for digital rights. As a member of the "Five Eyes", an intelligence-sharing partnership that facilitates the distribution of information acquired through surveillance, its surveillance regime has an impact far beyond its domestic borders.[18] Information collected under Australia's domestic surveillance laws is frequently handed over to other

governments with a history of overreach and abuse.[19] It also has an oversized impact in the Asia Pacific region.

How AI impacts human rights in Australia

With this troubling digital rights landscape in mind, we now examine the primary human rights impacted by AI in the Australian context.[20] The rights discussed are embodied in the three documents that form the foundation of international human rights law, the so-called "International Bill of Human Rights". These include the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social and Cultural Rights (ICESCR),[21] all of which Australia has ratified. To these we add the right to data protection as defined by the EU Charter of Fundamental Rights.[22] For each human right we discuss how current and prospective uses of AI and algorithmic decision making in Australia violate or risk violating that right. We then discuss the extent to which Australian law protects against potential rights violations.

Many of the human rights issues discussed below 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 too complex for humans to understand. Additionally, the harms facilitated by AI often disproportionately impact marginalised populations. The historic marginalisation of these groups is reflected in the

data used to train AI systems, and can result in outputs that entrench these patterns.

Rights to privacy and data protection[23]

Privacy is a fundamental right that is essential to human dignity, as it also enables other rights, such as the rights to freedom of expression and association.[24] Many governments and regions now recognise a fundamental right to data protection. Data protection is primarily about protecting any personal data related to you, and is closely tied to the right to privacy.[25]

By its very nature, AI threatens the rights to privacy and data protection. AI systems are trained through the analysis of huge data sets. Data are also collected to create feedback mechanisms that recalibrate and continually refine the AI model. When this data is about people, it clashes with the rights to privacy and data protection. Additionally, the analysis of data using AI systems can reveal private information about people, and can successfully re-identify individuals in a dataset that has been stripped of any personally identifying information.[26] Thus, non-person data points become sensitive even if derived from large datasets fed from publicly available information.

In Australia, the human rights most threatened by current uses of AI are the rights to privacy and data protection. There are two overarching reasons for this. First, the government's increasing institutionalisation of mass surveillance practices and lack of legal protections against overreach mean there is little to protect citizens against the government utilising AI to expand and refine its surveillance apparatus.

Second, the government has increasingly moved to centralise information into large databases as part of its broader initiatives to enable online government services, such as the myGov platform. A number of these initiatives have failed spectacularly, some with serious consequences for ordinary Australians caught in the middle.[27] The repeated bungling of technology projects suggest the government has a careless attitude toward privacy, and frequently fails to consider the potential risks of throwing technology on top of existing systems.[28]

With this in mind, the following cases represent major risks to the rights to privacy and data protection in Australia.

The planned national facial recognition system

AI's capacity to process and analyse multiple data streams in real time has expanded the scope of mass surveillance around the world, particularly though 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.[29] 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.[30] 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.[31]

The sale of cell phone location data to third parties

A 2018 investigation revealed that mobile provider Telstra was selling customers' location data to third parties without their knowledge or consent. Telstra stated the use of the information was consistent with its privacy policy, which states that customers' information could be shared with "our dealers, our related entities or our business or commercial partners and other businesses we work with".[32] Telstra also claims the data is anonymised, and that they do not share any information that "identifies or could reasonably identify a customer".[33] However, research has shown that location data alone can be used to accurately estimate a person's age, gender, occupation, and marital status.[34]

Does Australian law protect against the risks to privacy and data protection?

There is no affirmative right to privacy in Australia. Nor do Australians have the ability to file a lawsuit against an individual, entity, or the government for a violation of privacy. And while there is federal legislation related to privacy, it is full of loopholes and is woefully inadequate to the unique risks to privacy of the digital age.

The *Privacy Act* regulates the collection and use of personal information via a set of "Privacy Principles" that apply to most federal government agencies, as well as businesses and nonprofits with annual turnover of over $3 million, with some exceptions.[35] It defines personal information as "information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable".[36]

The Privacy Principles include a number of laudable provisions, such as requiring entities to inform individuals why their personal information is being collected, how it will be used, and to whom it will be disclosed, allowing individuals the option of not identifying themselves or using a pseudonym (with exceptions), mandating the collection of personal information "only if necessary", allowing individuals to request access to their personal information, as well as request the information be corrected if inaccurate.

Nevertheless, the *Privacy Act* has a number of shortcomings. First, it does not address the ability of AI to easily re-identify information that has been de-identified. Information in de-identified data sets does not qualify as personal information according to the definition, and therefore is not subject to any of the protections stipulated by the Privacy Principles. Second, there is no requirement for entities to obtain consent prior to collecting personal information.

This removes the right of individuals to decide whether or not they are comfortable with the entity's disclosed use of their data. Third, it does not apply to state or territory governments, although some states have passed their own privacy legislation. Fourth, it does not address the privacy threats of government surveillance. Although the *Privacy Act* covers the Australian Federal Police and CrimTrac, it does not cover most law enforcement and intelligence agencies, which arguably are the entities most likely to commit major breaches of privacy. Further, where it does apply to law enforcement agencies there are many exemptions and carve outs that allow for near limitless data collection.[37] And finally, the *Privacy Act* only provides for limited civil redress via a complaints mechanism overseen

by an Information Commissioner.[38] These gaps make the *Privacy Act* nearly useless in protecting Australians against the privacy and data protection risks posed by AI.

The *Data Sharing and Release Act*

One new piece of legislation would erode the already weak *Privacy Act* even further. As part of its modernisation efforts, the Australian government would like to be able to capitalise on all the data it collects.[39] The *Data Sharing and Release Act*, introduced in Parliament in mid 2018, seeks to make it easier for government agencies to share data with each other, allowing any government entity to access any and all the information the government holds about you, and also permitting the government to share data with "trusted" third parties and researchers.[40] While it is certainly good to use data analysis to create evidence-based policy, the proposed law includes no meaningful privacy and security protections.

Currently, such use of individuals' data potentially conflicts with the hundreds of existing data confidentiality provisions across existing Australian law, including the *Privacy Act* and the Privacy Principles. However, if passed, the *Data Sharing and Release Act* would override any conflicting legislation for both government and non-governmental entities alike.[41] Additionally, the bill would instate data sharing by default. There would be no ability for Australians to opt out of having their data shared across the government and with third parties.[42] With this bill, the government is clearly communicating its view that your data belongs to them, as well as continuing carelessness in its approach to risk management of technology projects.

Rights to freedom of expression, assembly and association[43]

Governments around the world have begun passing laws requiring internet companies to quickly remove problematic content, such as terrorist propaganda, hate speech, and so-called "fake news".[44] In the wake of the 2019 New Zealand mass shooting, Australia passed a law making content providers criminally liable if they fail to remove "abhorrent violent material expeditiously".[45] To comply with laws that demand quick removal in the face of steep penalties, companies have increasingly turned to AI to detect and automatically remove such content.

Despite the good intentions of these laws, they ultimately push companies to censor legitimate speech. Because the AI used to moderate content is imperfect, legitimate content is often mistakenly removed while not all problematic content is caught.[46]

Violations of the right to privacy have a chilling effect on free expression. When people feel they are being watched, or have been stripped of anonymity, they self-censor and alter their behavior. AI-powered surveillance only exacerbates this effect, which will have serious repercussions for freedom of expression.[47] The planned national facial recognition system thus poses a major threat. For example, if used in public spaces to identify individuals at a protest, it could have a significant chilling effect on assembly, as many people rely on anonymity to feel safe gathering in public to express their views. This is compounded by the worrying trend of state and territory governments proposing anti-protest laws. These laws generally

include vague and poorly defined offenses, excessive police powers, harsh penalties, and the prioritisation of private sector interests over the right of individuals to protest.[48]

Does Australian law protect against the risks to expression, assembly and association?

Freedom of political expression and assembly are two of the few constitutionally protected rights in Australia. The High Court has ruled that "freedom of political communication" includes both verbal and non-verbal communication, such as public demonstrations and protests. It has also ruled that laws that severely restrict political communication are constitutionally invalid.[49]

It is unclear if those protections are sufficient to address the largely indirect threats posed by using AI for surveillance of protests. This is because surveilling of public demonstrations does not constitute a legal restriction of these rights. Therefore, the question of whether or not AI-enabled surveillance infringes upon the right to political communication will likely have to be litigated in the courts.

Rights to liberty and security, equality before the courts, a fair trial[50]

AI is increasingly utilised in criminal justice systems around the world, and Australia is no exception. The use of AI in this context often occurs in two different areas: criminal risk assessment — evaluating whether or not a defendant is likely to reoffend in order to recommend sentencing and set bail — or so-called "predictive policing", using insights from data to predict where and when crime will occur and direct law

enforcement action accordingly.[51] These tools are often created with good intentions. For example, to address the human bias of judges by providing them with "objective" suggestions based on data, or to better allocate scarce police resources. However, they often end up entrenching the very social biases they are designed to solve.

Criminal risk assessment software is pegged as a tool to merely assist judges or law enforcement. However, by rating a person as high or low risk of reoffending, they attribute a level of future guilt, which may interfere with the presumption of innocence required in a fair trial. [52] Reports suggest that judges know very little about how risk-scoring systems work, yet many rely heavily upon the results because the software is viewed as unbiased.[53] When they use these tools, government officials essentially hand over judicial decision making to the private vendors who developed them. The engineers at these vendors, who are not elected officials, use data analytics and design to code policy choices often unseen by both the government agency using the software and the public. When individuals are detained or given certain sentences for reasons they will never know and that cannot be articulated by the government authority charged with making that decision, trials may not be fair, there may be no equality before the law, and these rights may be violated.

Criminal risk assessment in New South Wales

New South Wales police have used such a tool in the policing and management of individuals as young as 11 years old. The "Suspect Targeting Management Plan" (STMP) is both a risk assessment tool that predicts the likelihood a person will

become a repeat offender, as well as a targeted predictive policing program meant to increase police contact with "high-risk" potential offenders to deter them from committing crimes. People entered into STMP are nominated by police, but the criteria for nomination are not publicly available. The system then calculates how likely the person is to commit a crime by classifying them into categories of extreme risk, high risk, medium risk, or low risk.[54] An investigation by the Youth Justice Coalition found that STMP disproportionately targets young people, and particularly Indigenous youth, who made up 44% of STMP targets.[55] Researchers were unable to obtain data about how an individual's risk category is determined. However, the operation of the system is likely to create a negative, self-reinforcing feedback loop that ultimately results in Indigenous youth becoming increasingly targeted by police. This only exacerbates existing inequities in policing and incarceration.

Currently, Indigenous Australians make up over 25% of the prison population, despite being only 2% of the total population.[56]

Risk assessment for asylum seekers at the border

In 2017, the government began using a risk assessment tool to assess the security risk posed by immigrants, from asylum seekers to those overstaying their visas, in immigration detention centres around the country. According to a spokesperson for the Department of Immigration and Border Protection, the Security Risk Assessment Tool (SRAT) uses information about the detainee's behaviour both during and prior to detention, as well as factors such as age and health. The risk score is then

used to determine what detention facility they are sent to, whether they require physical restraints, and whether they are allowed certain privileges. Immigrant rights advocates stated that the determinations of the system could not be challenged, and also complained it does not take mental health issues into account.[57] In a report following a visit to a detention centre, the Human Rights Commission found significant variation in the background and circumstances in detainees labeled as high risk, suggesting the software does a poor job of truly assessing security risk and may actually result in danger to detainees.[58]

Facial recognition in law enforcement

Law enforcement around the world is incorporating facial recognition into policing, and if the national facial recognition system known as The Capability is established, Australian police will likely follow suit. 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.[59] 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.[60]

Does Australian law protect against the risks to liberty, security, equality for the law and fair trial?

Most of Australian law governing security and detention is embedded in the criminal code. There are many laws that may allow arbitrary detention related to terrorism.[61] Section 189 of the *Migration Act 1958* requires unlawful non-citizens in the

migration zone to be placed in immigration detention.[62] Treatment of detainees is not prescribed by law, but rather is part of the internal instructions of the Department of Immigration and Citizenship, which provide guidance regarding the treatment of people in immigration detention under the *Migration Act 1958*.[63] There are therefore likely no legal protections that address risk assessment in immigrant detention centers.

There is also no right to a fair trial specified by law. Section 80 of the Constitution provides for the right to trial by jury; however, this is more of a procedural mechanism as it does not specify the nature of this right. Rather, fair trial procedures are built into the criminal procedures of the federal court.[64] Additionally, Australian law contains conflicting provisions regarding the presumption of innocence. Section 141 of the *Evidence Act 1995* provides that in a criminal proceeding, the court is not to find the case of the prosecution proved unless it is satisfied that it has been proved beyond reasonable doubt. Yet it also provides that the defendant's case is proven on the balance of probabilities.[65] This creates an uncertain landscape for legal protection against, for example, criminal risk assessment that violates the right to a fair trial.

Rights to equality and non-discrimination[66]

Discrimination is inherent in many current uses of AI. The models are designed to sort and filter, whether by ranking search results or categorising people into groups. This discrimination becomes problematic when it treats different groups of people differently. Sometimes this is justified; for example, in the case of affirmative action programs in universities.

However, other uses of AI are not. This discrimination is often the result of some form of bias in systems that perpetuate historical injustice in everything from prison sentencing to loan applications.

The use of the STMP likely violates the right to non-discrimination because it disproportionately targets Indigenous youth. Proponents of criminal risk assessment systems often justify them by alleging they are less discriminatory than human judges or police, and therefore result in more balanced outcomes. However, it is dangerous to assume that just because AI might be more accurate or less discriminatory than humans, it is necessarily "good". This view risks simply institutionalising machine bias under the guise of objectivity.

Additionally, 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.

Does Australian law protect against the risks to equality and non-discrimination?

The right to non-discrimination is well protected under Australian law. It is the only case in which Parliament elected to enact domestic legislation to implement its obligations under the various UN treaties.[67] These include the *Racial Discrimination Act 1975*, the *Sex Discrimination Act 1984*, the *Disability Discrimination Act 1984*, and the *Age Discrimination Act 2004*. All Australian federal anti-discrimination laws are

enforced through a two-step process: first, an individual lodges a complaint with the Human Rights Commission, which will investigate and attempt to resolve it via conciliation. A small percentage of cases then move to adjudication in the federal courts.[68] The robustness of Australian anti-discrimination law and its general compliance with international anti-discrimination law allows the Human Rights Commission to take a leading role in uncovering and dealing with discrimination issues. This will be particularly important related to potentially discriminatory uses of AI, because often individuals are unaware that an automated system is being used to inform decision making in discriminatory ways.

How should Australia address the human rights risks of artificial intelligence?

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 processes, 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.

The following recommendations, some of which Access Now made in its reports on human rights in the age of artificial intelligence and on the state of digital rights in Australia,[69] 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 institutionalising 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.[70] 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 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. Because data is the engine of AI, any law that mandates protection of personal data will necessarily implicate 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.[71]

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".[72]

6. Develop high standards for government use of AI.[73] 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.[74] 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.

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age. https://www.accessnow.org/

Endnotes

1 RightsCon.org
2 The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems, August 2018, https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf.
3 Human rights in the Age of Artificial Intelligence. *Access Now,* November 2018, https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf
4 Human rights in the Digital Era: an international perspective on Australia. *Access Now,* August 2018, https://www.accessnow.org/cms/assets/uploads/2018/07/Human Rights-in-the-Digital-Era-an-international-perspectiv e-on-Australia.pdf
5 Van Veen C, Artificial intelligence: What's human rights got to do with it? *Data & Society: Points*, May 14, 2018, https://points.datasociety.net/artificial-intelligence-whats-human-rights-got-to-do-with-it-4622ec1566d5
6 Zevenbergen B, Marrying ethics and human rights for AI scrutiny. *Considerati,* https://www.considerati.com/publications/blog/marrying-ethics-human-rights-ai-scrutiny/ .
7 See note 3, Human rights in the Age of Artificial Intelligence, for further discussion of the interplay between ethics and human rights in AI.

8 The Australian Constitution provides for just five rights: the right to vote, protection against the acquisition of property on unjust terms, the right to a trial by jury, freedom of religious observance, and a prohibition of discrimination on the basis of state of residency. In 1992, the High Court also recognised that the right of political communication is also constitutionally protected.
9 Victoria and the Australian Capital Territory both have human rights charters based on the International Covenant of Civil and Political Rights (ICCPR).
10 Human rights in Australia. Australian Human Rights Commission, https://www.humanrights.gov.au/education/students/get-informed/human-rights-australia
11 Chappell L et al., *The Politics of Human Rights in Australia*. Cambridge University Press: 2009, pp. 33–36.
12 These include the ICCPR, ICESCR, CRC, CEDAW, CERD, CRPD, and CAT. It also includes the First Optional Protocol of the ICCPR, which allows individuals to file written complaints to the UN Human Rights Committee if they believe their rights under the ICCPR have been violated and they have exhausted all domestic remedies.
13 The AHRC has begun thinking about its role in protecting human rights in the age of AI, and how it might promote responsible innovation. See https://www.humanrights.gov.au/our-work/rights-and-freedoms/publications/artificial-intelligence-governance-and-leadership for more information.
14 See note 4, Human rights in the Digital Era: An international perspective on Australia. *Access Now*.
15 Evershed N & Safi M, All of Australia's national security changes Since 9/11 in a timeline. *The Guardian*, October 18, 2015, https://www.theguardian.com/australia-news/ng-interactive/2015/oct/19/all-of-australias-national-security-changes-since-911-in-a-timeline.
16 The major surveillance laws include: *Telecommunications (Interception) Act 1979* (https://www.legislation.gov.au/ Details/C2018C00201); *Telecommunications Act 1997* https://www.legislation.gov.au/Details/C2018C00161); the *Surveillance Devices Act 2004* (ttps://www.legislation.gov.au/Details/ C2018C00188); The "Terror Laws" of 2014 and 2015 (https://www.accessnow.org/global-state-of-surveillance-australias-terror-laws-set-to-erode-human-righ/). On the anti-encryption law: https://www.wired.com/story/australia-

encryption-law-global-impact/, and https://www.accessnow.org/australia-joins-russia-and-china-in-undermining-users-security-and-threatening-human-rig hts/ including the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (https://www.legislation.gov.au/Details/C2015A00039).

17 *Internet Enemies Report 2012.* Reporters Without Borders, https://rsf.org/sites/default/files/rapport-internet2012_ang.pdf

18 The Five Eyes partnership includes Australia, the United States, United Kingdom, Canada and New Zealand.

19 See note 4, Human rights in the Digital Era: An international perspective on Australia. *Access Now*.

20 Although future uses of AI have the potential to impact many more internationally recognized human rights, we focused on those we believe most relevant to the Australian social, political and legal context. For a more comprehensive look at the human rights impacts of AI, see Access Now's report, *Human Rights in the Age of Artificial Intelligence.*

21 See https://www.ohchr.org/EN/ProfessionalInterest/Pages/InternationalLaw.aspx for more information

22 *Charter of Fundamental Rights of the European Union.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

23 Article 12 of UDHR, Article 17 of ICCPR, Article 8 of the EU Charter of Fundamental Rights

24 *Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance.* https://necessaryandproportionate.org/principles.

25 Masse E, Data protection: Why it matters and how to protect it. *Access Now,* January 25, 2018, https://www.accessnow.org/data-protection-matters-protect/.

26 Ohm P, Broken promises of privacy: Responding to the surprising failure of anonymization, *UCLA Law Review, 57,* 1701 (2010), https://www.uclalawreview.org/pdf/57-6-3.pdf.

27 A recent Senate Committee report on digital government services decried an "unprecedented litanty of failure" of various technology projects, from Robo-debt, to the 2016 online census failure, to the suspension of the Australian Criminal Intelligence Commission Biometric Identification Services project. See Smith P, Government rejects Senate report that slams "unprecedented" tech failures. *Financial Review*, June 28, 2018, https://www.afr.com/technology/

government-rejects-senate-report-that-slams-its-unprecedented-tech-failures

28 One high-profile example of this is the Robo-debt scandal, in which the automation of the welfare compliance in 2016 via a poorly constructed algorithm falsely claimed that tens of thousands of Australians owed the government overpaid welfare funds, some amounting nearly $100,000. Subsequent analysis conservatively estimated the robo-debt system's error rate was 20%, and despite the scandal and the 29 million unanswered calls to CentreLink, the program was not shut down until the Senate ordered it over a year later. See https://logicmag.io/03-austerity-is-an-algorithm/

29 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

30 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

31 Locker M, 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

32 Whyte S, Telstra's new sales pitch: your location, hour-by-hour. *The Sydney Morning Herald*, March 4, 2018, https://www.smh.com.au/national/telstra-s-new-sales-pitch-your-location-hour-by-hour-20180430-p4zch2.html

33 Ibid.

34 Bellovin SM et al., When enough is enough: Location tracking, mosaic theory, and machine learning. *NYU Journal of Law and Liberty,* 2014, 8(2), 555–628, https://digitalcommons.law.umaryland.edu/fac_pubs/1375/

35 The following businesses are subject to the *Privacy Act* regardless of their size: private sector health providers, businesses that sell or purchase information, credit reporting bodies, and government contractors.

36 Privacy Law, Office of the Australian Information Commissioner, https://www.oaic.gov.au/privacy-law/

37 The Parliamentary Joint Committee on Law Enforcement released a report in April 2019 on the impact of new and emerging technology. One of their recommendations for the government to consider when developing any future strategies for biometric data and facial recognition systems is to "publicly releasing additional technical information about the nature of the facial matching scheme, and the process for ensuring that there are not false matches, in order to inform the public about its operation and to allow informed debate about its use and future database links". See https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/NewandemergingICT/Report for more information.

38 State of Digital Rights. *Digital Rights Watch*, May 2018, https://digitalrightswatch.org.au/wp-content/uploads/2018/05/State-of-Digital-Rights-Web.pdf.

39 *New Australian Government Data Sharing and Release Legislation: Issues paper for consideration.* Department of the Prime Minister and Cabinet, 4 July 2018, https://www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation.

40 Warren J, Data sharing and release issues. *eigenmagic,* July 30, 2018, https://www. eigenmagic.com/2018/07/30/tljr-data-sharing-and-release-issues/

41 Williams R, The *Data Sharing and Release Act* is coming for your data. *Independent Australia*, August 7, 2018, https://independentaustralia.net/life/life-display/-the-data-sharing-and-release-act-is-coming-for-your-data,11761

42 Australians have recently shown they are skeptical of data centralisation initiatives. As of February 2019, 1 in 10 Australians eligible for Medicare had opted out of the new My Health Records system. See https://www.theguardian.com/australia-news/2019/feb/20/more-than-25-million-people-have-opted-out-of-my-health-record for more information

43 Article 19 of the UDHR and Article 19 of the ICCPR; Article 18 of the ICCPR and UDHR, Articles 21 and 22 of the ICCPR, Article 20 of the UDHR

44 A Freedom House survey found 30 of 65 of governments attempted to control online discussions. https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy

45 How tough new Australian social media law works. *Sydney Morning Herald*, April 5, 2019, https://www.smh.com.au/world/oceania/how-tough-new-australian-social-media-law-works-20190405-p51b15.html
46 Nolasco D & Micek P, Access Now responds to Special Rappoteur Kaye on "Content Regulation in the Digital Age". *Access Now,* January 11, 2018, https://www.accessnow.org/access-now-responds-special-rapporteur-kaye-content-regulation-digital-age/
47 Privacy International and Article 19, "Privacy and Freedom of Expression in the Age of Artificial Intelligence". April 2018, https://privacyinternational.org/report/1752/privacy-and-freedom-expression-age-artificial-intelligence
48 Say it loud: Protecting protest in Australia. Human Rights Law Center, December 13, 2018, https://www.hrlc.org.au/reports/say-it-loud.
49 Ibid.
50 Articles 3, 6, 7, 8, and 10 of UDHR, Articles 9 and 14 of the ICCPR.
51 For more information and a case study of AI used in the criminal justice system in the United States, see Angwin et al., Machine bias. *ProPublica*, May 23, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
52 According to the General Comment 32 on Article 14 of the ICCPR
53 See note 51, Angwin et al., *Machine Bias.*
54 Lieu J, Australian police use a secret algorithm and blacklist to target children suspected of reoffending. *Mashable*, October 16, 2017, https://mashable.com/2017/10/26/children-predictive-policing-australia/
55 Vicki S & Padolfini C, Policing young people in NSW: A study of the Suspect Target Management Plan. Youth Justice Coalition, October 25, 2017, https://apo.org.au/node/116176
56 Prisoners in Australia. Australian Bureau of Statistics, June 12, 2018, https://www.abs.gov.au/ausstats/abs@.nsf/Lookup/by% 20Subject/4517.0~2018~Main%20Features~Aboriginal%20a nd%20Torres%20Strait%20Islander%20prisoner%20characteristics%20~13
57 Bagshaw E & Kozoil M, Computers replace humans in assessing danger of inmates in immigrant detention. *The Sydney Morning Herald*, August 26, 2017, https://www.smh.com.au/politics/federal/computers-replace-humans-in-assessing-danger-of-inmates-in-immigration-d etention-20170825-gy4i19.html.

58 *Australian Human Rights Commission Inspection of Christmas Island Immigration Detention Centre: Report.* Australian Human Rights Commission, August 2017, https://www.humanrights.gov.au/sites/default/files/document/publication/AHRC_2018_CIIDCinspection_report.pdf

59 Lohr S, Facial recognition is accurate, if you're a white guy. *New York Times,* February 2, 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

60 Goode L, Facial recognition software is biased towards white men, researcher finds. *The Verge*, February 11, 2018, https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error.

61 For example, division 105 of the *Criminal Code Act 1995,* which authorises the preventative detention order where it is reasonably necessary to detain a person to prevent a terrorist act. Division 3 of Part III of the *Australian Security Intelligence Organisation Act 1979* provides for the issuing of a "questioning and detention warrant" authorising a person to be questioned by ASIO and detained by a police officer, where the issuing authority is satisfied that this will substantially assist the collection of intelligence important in relation to a terrorism offense.

62 Right to security of the person and freedom from arbitrary detention. Attorney General's Department, https://www.ag.gov.au/RightsAndProtections/HumanRights/Human-rights-scrutiny/PublicSectorGuidanceSheets/Pag es/Righttosecurityofthepersonandfreedomfromarbitrarydetention.aspx#6whcih

63 Right to human treatment in detention. Attorney General's Department, https://www.ag.gov.au/RightsAndProtections/HumanRights/Human-rights-scrutiny/PublicSectorGuidanceSheets/Pages/RighttohumantreatmentindetentionaspX

64 Fair trial and fair hearing rights. Attorney General's Department, https://www.ag.gov.au/RightsAndProtections/HumanRights/Human-rights-scrutiny/PublicSectorGuidanceSheets/Pag es/FairtrialandfairhearingrightsaspX#6which

65 Presumption of innocence. Attorney General's Department, https://www.ag.gov.au/RightsAndProtections/HumanRights/Human-rights-scrutiny/PublicSectorGuidanceSheets/Pages/PresumptionofinnocenceaspX#6which

66 Articles 3, 26 and 27 of the ICCPR. Article 3 of the ICESCR.

67 These include the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), Convention on the Rights of Persons With Disabilities, among others.

68 Gaze B & Hunter R, *Enforcing Human Rights: An Evaluation Of The New Regime.* Themis Press: 2010.

69 See note 3, Human rights in the Age of Artificial Intelligence and note 4, Human rights in the Digital Era: An international perspective on Australia, *Access Now.*

70 Necessary and Proportionate Principles.

71 See https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf

72 Knaus C, 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-t hat-allows-it.

73 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/

74 See https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf