New South Wales
Council for Civil Liberties

NSWCCL SUBMISSION

AUSTRALIAN HUMAN RIGHTS COMMISSION

HUMAN RIGHTS AND TECHNOLOGY

DISCUSSION PAPER

5 March 2020

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Contact NSW Council for Civil Liberties

http://www.nswccl.org.au
office@nswccl.org.au
Street address: Level 5, 175 Liverpool Street, Sydney, NSW 2000, Australia
Correspondence to: PO Box A1386, Sydney South, NSW 1235
Phone: 02 8090 2952
Fax: 02 8580 4633

HUMAN RIGHTS AND TECHNOLOGY - DISCUSSION PAPER

Introduction

The NSW Council for Civil Liberties (*NSWCCL*) thanks the Australian Human Rights Commission for the opportunity to comment on the December 2019 Discussion Paper concerning Human Rights and Technology.

NSWCCL endorses the proposals set out in the Discussion Paper. The Commission invites stakeholders to comment on the proposals and questions in this Discussion Paper and NSWCCL comments will be confined to sections of Parts A, B and C. NSWCCL has also collaborated with other civil society groups in providing a broader joint submission to the ALRC for this Inquiry.[1]

NSWCCL agrees that safeguards are necessary to ensure that the liberties and rights of Australians are not unreasonably curtailed by surveillance and AI decision-making technology. As a society we need to avoid the possibility that people feel unable to go about their normal business because they are constantly being watched or tracked. In terms of personal private information, once collected, used and stored, by third parties, it becomes increasingly difficult to protect and regulate its use. Often that personal private information is collected or used in a manner that is without the knowledge, or consent, of the individual.

1. Proposal 1: National Strategy on New and Emerging Technologies that promote effective regulation

It is acknowledged, in the Discussion paper ,that laws protecting individuals against breaches of their privacy rights, have not kept pace with technology. Surveys have shown that community trust in new and emerging technologies has been decreasing, for example, with most Australians concerned about their online privacy.[2]

Australian government policy, on new technology, has tended towards self-regulation which is also, inevitably, fragmented. The Australian Productivity Commission noted that "Australia's legal and policy frameworks for collection, storage and use of public- and private-sector data are ad hoc and not contemporary, and that, as a result, Australia is not participating in developments in the use of data or benefiting from data-driven services and efficiencies". It has called for fundamental, systematic change in the way governments, businesses and individuals handle data.[3]

---

[1] See Submission made jointly by the Australian Privacy Foundation, the Queensland Council for Civil Liberties, Liberty Victoria, Electronic Frontiers Australia and the New South Wales Council for Civil Liberties.
[2] Goggin, G., Vromen, A., Weatherall, K., Martin, F., Webb, A., Sunman, L., & Bailo, F. (2017) Digital Rights in Australia *Departments of Media Communications, and Government and International Relations, Faculty of Arts and Social Sciences, and the University of Sydney Law School, University of Sydney.* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090774 >accessed 25 Feb 2020
[3] Australian Productivity Commission (2017) Data Availability and Use Report, p. 12 in Goggin, G., Vromen, A., Weatherall, K., Martin, F., Webb, A., Sunman, L., & Bailo, F. (2017) Digital Rights in Australia *Departments of Media Communications, and Government and International Relations, Faculty of Arts and Social Sciences, and the University of Sydney Law School, University of Sydney.* pp21-22 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090774 >accessed 25 Feb 2020

NSWCCL agrees that the substance of Article 22 of the EU General Data Protection Regulation (*GDPR*), should be adopted by Australian legislators, as best practice in protecting individuals in the case of automated decision-making. Article 22 of the GDPR provides for the right not to be subject to a decision based solely on 'automated processing, including profiling' with legal or significant impact.

Such legislation should be supported by an enforceable human rights framework such as a Bill of Rights. Australia is one of the few Western democracies that lacks such a framework.

Australia needs to regulate how new and emerging technologies are developed; in what contexts they should be monitored and to ensure that there is independent oversight of operation processes. Australians need both adequate protection from adverse impacts and the ability to properly enforce their legal rights.

Recommendation 1

NSWCCL endorses a national strategy on new and emerging technologies that promotes effective regulation, consistent with Article 22 of the GDPR.

Recommendation 2

NSWCCL recommends that a national Bill of Rights or similar legal framework be enacted to support human rights of Australians affected by new and emerging technologies.

Recommendation 3

NSWCCL recommends that legislation be enacted to ensure privacy protection and security in relation to new and emerging technologies which includes both adequate protection from adverse impacts to individuals and properly enforceable legal rights.

2. Proposal 4: Statutory cause of action

NSWCCL supports a limited statutory cause of action to sue for serious breach of privacy, where there is a reasonable expectation of privacy. The existing privacy legislation at Commonwealth and State levels does not provide protection, or remedy, for many kinds of invasion of personal privacy. The focus of existing legislation is on data protection. Related legislation in the fields of defamation, breach of contract, trespass and telecommunications, only cover some aspects of invasion of privacy and leave other gross breaches without remedy. Any cause of action needs to be broadly formulated to capture future forms of privacy infringement.[4]

In 2019, the Australian Competition and Consumer Commission recommended that a new statutory cause of action be created to cover serious invasions of privacy with the aim to reduce the "bargaining power imbalance" between individuals and digital platforms.[5]

---

[4] Witzleb, Normann (2011) A statutory cause of action for privacy? A critical appraisal of three recent Australian law reform proposals *19 Torts Law Journal 104-134* DOI: 10.13140/2.1.3159.1684

[5] Australian Competition and Consumer Commission (June 2019) Digital Platforms Inquiry- Final Report <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>

The arguments demonstrating the need for more effective protection of privacy, and for a statutory cause of action for serious invasion of personal privacy, have been extensively and repeatedly debated over the years.[6] These are outlined in the Discussion paper. A number of Law Reform Commissions have concluded that a statutory cause of action for serious invasion of privacy should be legislated in Australia and advised their governments accordingly.[7] However, there has been government inaction in the face of these, and other repeated recommendations, to undertake law reform.[8]

Recommendation 4

NSWCCL advocates:

- Legislation for a statutory cause of action for serious invasion of privacy to be drafted and enacted;
- The balancing of interests should constitute a separate defence;
- Protection of the public interest in freedom of expression must be appropriately recognised by at least:
  - inclusion of a limited definition of public interest in a non-exhaustive list of defences,
  - the limited definition of public interest to cover 'matters of concern to the public interest',
  - no blanket exclusions of journalists/media organisations from the ambit of the legislation
  - serious consideration for separate legislation for the right to freedom of expression including freedom of the press.

3. Proposal 5: Legislation requiring that an individual is informed where AI is materially used in a decision with legal or significant effect on the individual's rights.

The Council of Europe, Commissioner of Human Rights, considers that those who have had a decision made about them by a public authority, that is solely or significantly informed by the output of an AI system, should be promptly notified.[9] In the context of public services, especially justice, welfare, and healthcare, the individual user needs to be notified that an AI system will be interacting with them and that there is hasty recourse to a complaints person.

As AI operates at scale, without social control, its use in public or private sector decision-making must be notified in clear and accessible terms. Specific information about processing, purpose and the legal basis for processing, should be available to the individual whether that information is retrieved directly, or from other sources.

---

[6] See also NSW Council For Civil Liberties Submission on Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy (Nov 2011) <https://d3n8a8pro7vhmx.cloudfront.net/nswccl/pages/601/attachments/original/1418076925/2011_submission_serious_invasions_of_privacy.pdf?1418076925>

[7] These reviews resulted in three reports: New South Wales Law Reform Commission, Report 120, Invasion of Privacy (2009); (NSWLRC Report); Victorian Law Reform Commission, Surveillance in Public Places: Final Report 18, 2010; (VLRC Report) and the ALRC Report 108 in 2008.

[8] Daly, A. (2017). Privacy in automation: An appraisal of the emerging Australian approach. *Computer Law & Security Review: The International Journal of Technology Law and Practice,* in Goggin et. al., op. cit.

[9] Council of Europe Commissioner of Human Rights (May 2019) Unboxing Artificial Intelligence: 10to protect Human Rights https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

When AI decision making is involved, the giving of consent needs to be properly documented. That consent needs to be voluntary, specific and unambiguous;[10] not bundled consent, nor opt out. Any changes in use of the information collected or stored should prompt a requirement for renewed express consent.

Recommendation 5

NSWCCL supports legislation requiring that an individual is informed where AI in decision-making affects legal or significant rights of the individual.

Recommendation 6

NSWCCL recommends that express consent of the individual user be required, where AI decision-making is involved.

4. Question C: Does Australian law need to be reformed to make it easier to assess lawfulness of AI informed decision-making system, by providing better access to technical information used in AI-informed decision-making systems, such as algorithms?

NSWCCL endorses reform to more easily assess the lawfulness of AI decision-making. Accessing technical information used in decision-making or having open source AI are methods for doing so. Reform is particularly important, considering that the acts and practices of some Australian government agencies, including the intelligence agencies, are exempt from the *Privacy Act 1988.*[11]

For some time, Australian legislation has explicitly allowed computers to make important decisions previously made by ministers or staff. There remains little clarity about what decisions are being entrusted to computers. Australian Federal Court Justice Melissa Perry noted in a 2014 speech on the topic of automated decision-making in government that "[i]n a society governed by the rule of law, administrative processes need to be transparent and accountability for their result, facilitated".[12] Delegation of the government's decision-making process to AI should ensure in-built procedural fairness and effective and easily accessed appeal processes.

Incorrect or unfair decisions and lack of procedural fairness commonly result when computers replace a human decision maker. The Centrelink "Robodebt" fiasco demonstrates the significant harm that may be caused to individuals.[13] Many of these individuals were vulnerable welfare recipients who could not access the system or complaints process.

Organisations such as the Norwegian Data Protection Authority *(NDPA)* have maintained that data subjects should have the right to:

---

[10] The Norwegian Data Protection Authority (January 2018) Artificial Intelligence and privacy *Datatilsynet*, p.29

[11] S7 Privacy Act 1988

[12] Elvery, S. (2017) How algorithms make important government decisions — and how that affects you *ABC News* <http://www.abc.net.au/news/2017-07-21/algorithms-can-make-decisions-on-behalf-of-federal-ministers/8704858> Accessed 2019

[13] ibid

- access their information, with exceptions,
- rectify and delete information that is inaccurate or incorrect
- object to the processing of details and have the organisation cease to use that data unless there are compelling grounds to do so.
- demand limited processing, particularly where data is being processed unlawfully.[14]

The NDPA engages in algorithm risk assessment and this could be a role for the AI Safety Commissioner, as part of its monitoring powers when requesting algorithmic design details. (see point 6 below).

Recommendation 7

NSWCCL recommends the reform of Australian law to make it easier to assess the lawfulness of AI informed decision-making systems, by providing better access to technical information used in AI-informed decision-making systems.

Recommendation 8

NSWCCL recommends that any reforms in providing better access to technological information include easily accessed complaints and independent appeal processes, and remedies for the benefit for the individual user.

5. Proposal 11: A legal moratorium on facial recognition technology in decision-making that has a significant impact for individuals

NSWCCL supports the proposal for a legal moratorium on the procurement and use of facial recognition technology in decision-making. However, the moratorium should not be confined to facial recognition but all biometric technology that is able to identify an individual's physical and behavioural characteristics.[15]

It is accepted that the tolerance levels built into facial recognition systems (due in part to inconsistent human interpretation or misdescription) increases the identity error margin and consequent risk of inaccurate identifications.[16] Since the consequence of an individual being falsely accepted or rejected is potentially serious, accuracy and reliability need to be constantly assessed.[17] In many cases it is the homeless, poor and unemployed that are disproportionately affected by this kind of surveillance. The real effect of being surveyed

---

[14] The Norwegian Data Protection Authority op.cit. p.29

[15] The Economist (May 25th 2019) The Way you walk; see also NSWCCL (Nov 2018) Submission on Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018 <https://d3n8a8pro7vhmx.cloudfront.net/nswccl/pages/601/attachments/original/1418076925/2011_submission_serious_invasions_of_privacy.pdf?1418076925>

[16] White D, Dunn JD, Schmid AC, Kemp RI (2015) "Error Rates in Users of Automatic Face Recognition Software". *PLoS ONE*10(10): e0139827. <https://doi.org/10.1371/journal.pone.0139827>

[17] Australian Law Reform Commission (2008) Australian Privacy Law and Practice *ALRC Report 108*, paragraph 9.71 <https://www.alrc.gov.au/publications/report-108>; It is difficult to produce completely error-free results with biometric identity information, which may be due to differences at the time of data acquisition, like lighting and the equipment used. To accommodate for these factors, technicians generate a certain tolerance, decreasing systems accuracy. As an example, the FBI's algorithm has a tolerance of, at least, 15% - Solon, O (27 March 2017) "Facial recognition database used by FBI is out of control, House committee hears" The Guardian, accessed 18 November 2017<https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports> accessed 2019

then trends towards the elimination of any difference in our society, and that chilling effect that tends to ensure that individuals mask or control their behaviour.[18]

There are numerous examples of scope creep and covert surveillance in the application of facial recognition technology. During the Gold Coast Commonwealth games in 2018, facial recognition had so few specific targets that it was opened up for general policing.[19] Recent revelations that Clearview AI has sold facial recognition software to the US and Australian law enforcement officers, are alarming.[20] The New York Times analysed Clearview AI computer code including the potential to use augmented-reality glasses which would enable users to potentially identify every person they saw. "The tool could identify activists at a protest or an attractive stranger on the subway, revealing not just their names but where they lived, what they did and whom they knew."[21] Consent, of social media groups or the individuals affected, were not given for scraping of images.[22]

As mentioned in the discussion paper, San Francisco was one of the first major cities to ban local government agencies, including the police, from using facial recognition technology. Misuse, misidentification and system bias were some of the reasons for imposing the ban. Though, increasing wrongful stop and arrest and general opposition to technology that could strip privacy and reinforce inequity, were others.[23] Other cities in the US have followed suit.

Recommendation 9

NSWCCL supports a legal moratorium on all biometric technology in decision-making, that has a significant impact for individuals.

6. Proposal 19: Establishment of an AI Safety Commissioner

The NSWCCL supports the establishment of an AI Regulatory Body (or Safety Commissioner) with the role outlined in the Discussion paper. NSWCCL agrees that such a body should have the additional powers of detecting and investigating bias in algorithms, though through system audits and with the power of enforcement of legal rights.

The AI Regulatory Body should encourage research into making AI more privacy friendly. Privacy friendly AI systems can more easily comply with regulations, use anonymization techniques and explain how data is processed.[24] "[I]t's important for algorithm operators and

---

[18] Fyfe, N.R. & Bannister, J. (1996) City Watching: Closed Circuit Television Surveillance in Public Spaces *The Royal Geographical Society (with the Institute of British Geographers)* Vol. 28, No. 1, pp. 37-46 at 43.
[19] Queensland Privacy Commissioner Philip Green in Bavas, J (2019) Facial recognition system rollout was too rushed, Queensland police report reveals *ABC news* <https://www.abc.net.au/news/2019-05-06/australias-biggest-facial-recognition-roll-out-rushed/11077350> accessed 23 June 2019
[20] Ryan, H. (Feb 2020) Australian Police Have Run Hundreds Of Searches On Clearview AI's Facial Recognition Tool *Buzz Feed News*< https://www.buzzfeed.com/hannahryan/clearview-ai-australia-police> accessed 1 March 2020
[21] Hill, K. (Jan 2020) The Secretive Company That Might End Privacy as We Know It *The New York Times*<https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> accessed 2 March 2020
[22] ibid
[23] Ghaffary, S (2019) San Francisco's facial recognition technology ban, explained *Vox* https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained accessed May 2019
[24] The Norwegian Data Protection Authority op.cit. p.28

developers to always be asking themselves: Will we leave some groups of people worse off as a result of the algorithm's design or its unintended consequences?"[25] Processing therefore requires transparency and this can be achieved by providing subject individuals with general information about process details.

Developer's complain that providing process details and code infringes intellectual property rights or reveals commercial secrets. Therefore, a key role for an independent body is auditability, enabling the assessment of algorithms, data and design processes. The Regulatory Body, given the appropriate expertise, should be able to keep intellectual property confidential and yet recognise where algorithms reinforce social differences and discrimination.[26]

The Regulatory Body should be tasked with supervising compliance with data protection regulations by government and the private sector. [27] The powers invested in the body, like European models, should include investigation and access to premises and data processing equipment, for the purposes of compliance with regulations. There should be authority to impose a fine and/or a ban on processing. [28]

Recommendation 10

NSWCCL supports the establishment of an AI Safety Commissioner with the additional powers of detecting and investigating bias in algorithms and enforcement of legal rights.

This submission was prepared by [redacted] on behalf of the New South Wales Council for Civil Liberties, with research assistance from [redacted]. We hope it is of assistance to the Australian Human Rights Commission.

Yours sincerely,

[redacted]

Secretary
NSW Council for Civil Liberties

Contacts in relation to this submission: Co-Convenors of NSWCCL Privacy Action Group, [redacted]

[25] Nicol Turner Lee, Paul Resnick, and Genie Barton, "Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms," *The Brookings Institution,* May 22, 2019 in Kerry, C.F. (Feb 2020) Protecting Privacy in an AI driven world *The Brookings Institution's Artificial Intelligence and Emerging Technology (AIET) Initiative* < https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/#footnote-20> accessed 3 March 2020

[26] The Norwegian Data Protection Authority op.cit. p.24

[27] Shaping Europe's digital future -Report/Study (8 April 2019) Ethics guidelines for trustworthy AI <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>

[28] The Norwegian Data Protection Authority op.cit.p.23