From: Australian Human Rights Commission
To: tech
Subject: Webform submission from: Human Rights and Technology > Body bottom elements
Date: Tuesday, February 25, 2020 5:25:26 PM

Submitted on Tue, 02/25/2020 - 17:25

Submitted by: Anonymous

Submitted values are:

Name
Terry Aulich

Address
[redacted]

Email address
[redacted]

Telephone number
[redacted]

Is this submission presented on behalf of an organisation:
No

I have read the information about this Project concerning publication, confidentiality, and privacy obligations at https://www.humanrights.gov.au/submission-policy
Yes

My submission is:
Public

Enter your response in the box below
SUBMISSION TO THE HUMAN RIGHTS COMMISSION ENQUIRY ON HUMAN RIGHTS AND TECHNOLOGY
FROM Hon Terry Aulich
1. Background
The Hon Terry Aulich is a former Tasmanian State Minister and Australia Senator and now chairs Aulich & Co, a strategic advisory company specializing in privacy and its relationship to new technology.
He was a former chair of the Joint Parliamentary Enquiry into the Australia card which led to the creation of the Privacy Commissioner, the Privacy Act and various anti-fraud measures such as the Tax File Number, 100 points bank ID system, birth and death certificate strengthening and the transaction limitations on money transfers.
He is currently chair of the privacy committees of the Biometrics Institute (London and Sydney) and the Association of Marketing and Social Research Organisations (AMSRO) and the Code Authority (probity committee) of Clubs NSW.
In his capacity as chair of the Biometrics Institute's privacy committee he drafts the biennial upgrades of the Institute's Biometric Privacy Guidelines.
This submission is made in a private capacity.
2. This Submission in Brief
2.1 New technology, especially Artificial Intelligence (AI) has the potential to significantly disrupt social cohesion unless there are processes built in to protect privacy, civil liberties and human rights.
2.2 AI is morally neutral so therefore the humans that plan, implement and manage its use must be central to the decision making, including fixing inaccuracies or decisions that are unfair, damaging, discriminatory or a cause of oppression. Prompt redress and the right for the aggrieved to challenge must exist, taking into account security or legal requirements.
2.3 Governments must be the moral leaders or model citizens for any new technologies that they use or are used by their proxies such as privatized organisations or those that provide a service on behalf of governments.

2.4 A Bill of Rights would help to ensure citizen rights in relation to the way new technologies are used. Since the current Government is bringing in legislation to specifically protect religious beliefs it would be of value to consider including a religious provision if required at all, in a comprehensive Bill of Rights.
2.5 Failing a Bill of Rights, Governments and their proxies should always have a publicly displayed ethics codes which essentially incorporates the critical concept that" just because you legally can do it, does that make it ethically or morally right?"
2.6 Governments need to promote the effective dissemination of Codes or Best Practice Guidelines that lift the standard of privacy protection and human rights concerns in both government and non-government organisations. Organisations such as the Association of Marketing and Social Research Organisations and the Biometrics Institute have longstanding and robust privacy and ethical Guidelines and Codes in place.
2.7 The Privacy Act should be amended to incorporate political parties, some small business and the media. The current exemptions of most small businesses, media and political parties needs to be reconsidered so that they are all included since they are significant trend setters in privacy and human rights matters.
2.8 Although AI has many benefits, the legal framework relating to it has many holes in it and has so far been unable to keep pace with the innovation and business velocity of AI. Whether it is drones or matching in facial recognition systems, the efficacy, efficiencies and business case of AI driven technologies is compelling.
2.9 AI like any technology is often most disturbing when humans have relinquished control and do not conduct proper risk assessments, monitoring and reviews of the AI system. This paper has indicated just a few instances where new technologies have failed because that preparatory work of testing, planning, monitoring and reviewing has been inadequate and open-ness has been avoided.
2.10 Technology is not perfect since the algorithms work best when they are trained and tested on the widest and deepest set of data collected from people. Therefore, absolute reliance on AI without other back-ups and/or evidentiary contexts is not recommended.

3. Purpose of this Submission
This submission is made as a private individual but obviously draws on the experience outlined in section one of this submission.
The Commission has logically asked for submissions in the final round that concentrate primarily on the sometimes vexed questions of regulation, accessibility and AI informed decision making.
This submission deals mainly with the question of AI informed decision making since the world is at a watershed in the roll out of AI driven technology which will have an even more profound impact in the very near future as AI technology rapidly achieves sophisticated levels of performance which may effectively prohibit appropriate human controls. An example of this will be the capacity of AI to make decisions based on an algorithm regime which will be close to impossible for humans to understand how that AI decision making occurred.

4. The Most Critical requirement to Manage AI
4.1 Humans Must be in Charge
The most significant issue is to ensure at this point in AI development that suitably qualified humans are in charge at the most critical phases of the AI decision making processes. Both human and machines are capable of error but, in terms of ensuring that privacy, human rights and other socially positive values are protected, it is vital that humans are involved at all stages of the process ie at planning, implementation, ongoing management and review stages. At the planning stage, there must be open and sometimes difficult assessments made about the accuracy, efficacy and social impact of the AI project and the human decision making associated with the project. Unforgivable failures such as the Robodebt scheme occur because of:
• Failures in the design of the technology and processes
• A failure to understand the potential weaknesses of technology,
• The unwillingness for Government to learn ie to accept that 20% of cases was assessed unfairly or a refusal to monitor faults in the processes and the system,
• A failure to acknowledge weaknesses in the system and to provide ready redress.
• A failure to understand that the technology and system was discriminatory in that it placed unfair, onerous and, in some cases impossible burdens of proof, often on vulnerable people.
• An unwillingness to review the effectiveness and stated objectives of the system and its effects on people caught in the system.
4.2 Comprehensive Privacy and Human Rights Planning Must Be Built into All Projects
The above problems have been a feature in one way or the other in the last Census where a Privacy impact Assessment, hastily done, failed to persuade the Australian Bureau of Statistics that a new process of conducting an online Census coupled with the new process of maintaining personal identifiable details of the respondents

was a high risk project. Most of the ultimate problems which caused significant reputational damage to ABS could be sheeted home to the planning process.

4.3 Qualified and Constantly Available Qualified Humans Must Manage the Process

Similarly, technology was involved in the case of Hakeem al-Araibi, the Bahraini soccer player who was mistakenly identified on an INTERPOL watch list and incarcerated in Thailand. Human intervention appears to have been absent at a critical phase of the process i.e no Australian in the AFP, acting for INTERPOL was able in a timely manner to check the simple fact that the Bahraini Government was not entitled to have an INTERPOL red notice raised against an Australian resident who was considered a refugee from Bahrain. It took a sustained campaign by former Socceroos champion Craig Foster to have Hakeem released after many months in detention; it is a moot question as to whether or not anyone with a lower profile would have been released back to Australia.

4.4 The Rights of People to Challenge and Seek Redress Must be Central

A major issue is the need to build into any planning, implementation and ongoing management process the right to challenge unfair decisions, inaccurate matching (for example, of similar names but different people) or discriminatory decision making. Seeking redress should be relatively easy, prompt, sensitively handled and the challenge and redress procedures easy to find on an organisation's website or public notices.

This issue of challenge and redress is increasingly significant given the expanding powers of security authorities to detain, raid or monitor Australian citizens and the capacity for bad actors to steal or misuse innocent persons' identities. If one misused SIM card is sufficient to cause an arrest and detention, the consequences for innocent individuals may be severe.

4.5 Governments Must Be Models of Moral Behaviour For All Those With Whom They Connect.

There is a vital need for Australian Governments, including local government to act as model citizens in how they plan, implement and manage new technology. Understandably, many governments seek to make savings, efficiencies or even revenue from new technologies. Parking fines and meters for example are significant revenue raisers for local government. But for example in Hobart, the Hobart City Council fines people for overstaying even when their ticket indicates that the meter has not expired yet. The council's excuse is that the ticket is only an indication and that the new high technology sensors are the determinant of the time the vehicle has been parked on that bay. There is no sign to indicate that this is the process nor are parking fines forgiven. This and other new technologies do breach the moral trust that citizens must have in their relationship with all governments. With social media, that breach of moral trust is now publicized more widely than before.

4.6 Governments Must Use Moral Suasion With Those It Can Influence in Terms of Protecting Privacy and Human Rights.

Part of the model citizen responsibilities required of Governments is the need to use moral suasion to positively affect the behaviour of organisations that connect with it. Connecting with government covers the act of conducting business with or providing services on behalf of government. In an age of outsourcing and privatization, that responsibility of moral suasion has become more critical in ensuring the strengthening of civil society.

4.7 Governments cannot outsource responsibilities for privacy protection, human rights and accountability.

Governments must be ultimately responsible for non-government proxies tasked with the provision of government or de facto government services. In the planning stage there must be contractual obligations specifically built in, at the implementation stage there has to be reporting, monitoring, accountability, redress and other end user/client protections built in and contracts should be reviewed and terminated or the miscreant proxy fined if privacy and other human rights are abused.

4.8 A Bill of Rights Would Help Protect Citizen Privacy and Human Rights.

Governments can assist the above processes if they were prepared to introduce an Australian Bill of Rights. This would be complex and sometimes awkward, even acrimonious but like the Australia Card debate which was conducted openly and honestly for over a year, the outcome would benefit all Australians and raise the moral and practical standards of Australian governments and the way they deal with their citizen's rights.

4.9 The Privacy Act Must Be Amended to Protect Privacy as a Human Right.

The current exemption of most small businesses, the media and political parties from the Privacy Act must be amended so that these major player and trend setters have a statutory requirement to protect privacy and other human rights. Small business, especially in the high tech area are often sub-contractors for larger companies and that has helped to create an ambivalent privacy regime even on some major IT projects. Many of them have core coding, diagnostic or algorithmic expertise that should only be used within a strong and accountable IT environment. Political parties have shown that they can use AI in ways that are totally lacking in transparency, are capable of collecting personal data, of disseminating lies and anti-social messaging to targeted individuals and are open to manipulation by bad actors on the political scene. Most Australians would be astonished to find how much political parties know about them and how systematically they are targeted by those parties with messaging specific to individual citizens. Worse still is the fact that political parties often engage volunteers or

consultants who have little or no understanding of privacy considerations.

4.10 A central requirement for authorities is to not to have blind trust in technology.

The Chamberlain case and cases in military operations have shown that expert witnesses or seemingly perfect matches can be misleading unless they are interpreted in their full context. Although this statement refers to DNA matching that was interpreted out of context, there are other situations where the technology has suffered some problems with environments such as poor lighting, inadequate and unrepresentative training of the algorithms leading to procedural unfairness and inaccuracies or bias. It should be noted that, for example, in facial recognition systems the algorithms are trained to be more accurate and efficient by the size and quality of the samples collected. Thus, China for example, which has few privacy inhibitions can train its algorithms on a much wider number of its citizens.
Further, Facebook and other social media have the potential for bad actors to harvest biometric images of people without their approval or with their approval based on a limited understanding of the technology and consequences. Whether Facebook et al actually do this or permit others to do it, is a matter of contention.

5. REFERENCES

Biometrics Institute's Biometrics Guidelines www.biometricsinstitute.org
Association of Market and Social research Organisations (AMSRO) www.amsro.com.au

6. CONTACT

[redacted]

The results of this submission may be viewed at:
http://www.humanrights.gov.au/admin/structure/webform/manage/submission_form_tech_2019/submission/7534