Dr Jenny Ng
Sender's Address: -
[redacted].

Submission to the Discussion Paper on Human Rights and Technology
Written by: Dr Jenny Ng

The following is my submission to the Discussion Paper on Human Rights and Technology. This submission is written in my personal capacity. It discusses the following issues which are related to the proposals in the Discussion Paper on Human Rights and Technology:

- An introduction of a statutory cause of action for serious invasion of privacy[1]
- Introducing Australian legislation for a 'Right to explanation' on automated decisions[2]
- Algorithmic Accountability and Impact Assessments [3]
- Biometric Recognition Regulation[4]
- Algorithmic Transparency[5]; and
- Task Forces or Commissions[6]

An introduction of a statutory cause of action for serious invasion of privacy[7]

There is a need for the statutory cause of action for serious invasion of privacy due to a lack of efficient legal avenue of redress for data breach issues. The *Privacy Amendment (Notification of Serious Data Breaches) Act 2017 (Cth)* makes it mandatory for a regulated entity to inform the Office of the Australian Information Commissioner (OAIC) and the affected individuals of a serious data breach. However, it would be difficult for victims of data breaches to bring an action in court for a breach of privacy as there is no tort of privacy in Australia.

In the report, *For Our Information, Australian Privacy Law and Practice*, the Australian Law Reform Commission (ALRC) recommended the introduction of a statutory cause of action for serious invasions of privacy. In 2014, the ALRC in the report, *Serious Invasions of Privacy in the Digital Era,* proposed a statutory cause of action which would enable Australians to bring an action in court for a breach of privacy.

However, individuals can make a representative complaint to the Office of the Australian Information Commissioner for such data breaches pursuant to section 38 of the *Privacy Act 1988 (Cth)*. These complaints are often in the form of class actions. There has been little success in making such complaints as it requires that the victims prove that 'harm' had been caused, rather than the fact that the victims had experienced embarrassment, anger or unhappiness. This

[1] relevant to proposal 4
[2] relevant to proposals 5 and 7; and Question B
[3] relevant to proposals 6, 8, 10, 12, 14, 15 and 18
[4] relevant to proposal 11
[5] Relevant to Question C
[6] relevant to proposals 13 and 17
[7] relevant to proposal 4

was illustrated in class actions such as the *Cbus class action.*[8]

It is noted that the *NSW Ambulance class action* fared better as it was able to reach a settlement that the plaintiffs seem agreeable to. However, it was a difficult process and highlighted the need for reforms in this area of the law. According to the solicitor for the lead plaintiff, Adjunct Professor George Newhouse, "This is the first privacy class action in Australia - it's the first to go to court and it's the first to settle in this way,"[9] However, he also stated that, "… it was a long and difficult road to travel. Our politicians need to intervene urgently and provide individuals with a satisfactory remedy for breaches of privacy and data breaches. If those who held our data were able to be held accountable for its misuse, then perhaps they would be more careful."[10]

Introducing Australian legislation for a 'Right to explanation' on automated decisions[11]

Data protection laws are foundational to new types of algorithmic activity.[12] Margot E. Kaminski and Gianclaudio Malgieri argued (in relation to the GDPR) that Data Protection Impact Assessments are a bridge between 'the two faces of the GDPR's approach to algorithmic accountability: individual rights and collaborative governance'.[13] However, it remains unclear whether such GDPR-style frameworks can or should offer a 'right to explanation' on automated decisions. Some have argued that such a right does not exist in the GDPR[14] On the other hand, some have also argued that the combination of several provisions in the GDPR can be used to obtain information on the decision-making processes in automated decisions.[15]

While Australia does not take the GDPR approach, and has its own legislative framework (albeit one which may be in need of reform due to a lack of a statutory cause of action for serious invasion of privacy),[16] Margot E. Kaminski and Gianclaudio Malgieri's views are useful as it highlights the importance of Data Protection Impact Assessments in bridging the gap between securing individual rights and achieving collaborative governance in algorithmic accountability. I think future Australian legislation should include Data Protection Impact Assessments in ensuring that there is a 'right of explanation' on automated decisions.

[8] *PB' and United Super Pty Ltd as Trustee for Cbus (Privacy)* [2018] AICmr 51

[9] McCubbing, Gus, 'NSW ambos win $275,000 class action payout after major data breach' *The Sydney Morning Herald* 10 December 2019

[10] Dolor, Sol, 'Court accepts settlement in pioneering privacy class action in Australia over data breach.' *Australasian Lawyer* 11 December 2019

[11] relevant to proposal 5 and 7; and Question B

[12] Frank Pasquale, 'The Second Wave of Algorithmic Accontability', *Law and Political Economy*, November 25, 2019, https://lpeblog.org/2019/11/25/the-second-wave-of-algorithmic-accountability/

[13] Margot E. Kaminski and Gianclaudio Malgieri, 'Algorithmic Impact assessments under the GDPR: Producing Multi-layered Explanations,' *U of Colorado Law Legal Studies Research Paper* No.19-28

[14] Sandra Watchter, Brent Mittelstadt, and Luciono Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,' *International Data Privacy Law*, December 28, 2016.

[15] Andrew Selbst and Julia Powles, 'Meaningful information and the Right to Explanation,' *International data Privacy Law* 7, no. 4 (November 27, 2017): 233-242

[16] see discussion above in relation to proposal 4

Indeed, the legislation and processes within the Data Protection Impact Assessments should allow an individual to request for reasons for the decision in ‘a non-technical explanation of the AI-informed decision, which would be comprehensible by a lay person, and a technical explanation of the AI-informed decision that can be assessed and validated by a person with relevant technical expertise’.[17] If the Data Protection Impact Assessment’s process is adopted, any person who is responsible for an AI-informed decision should provide a reasonable explanation for that decision, and if he fails to do so, Australian law should impose a rebuttable presumption that the decision was not lawfully made.[18]

Algorithmic Accountability and Impact Assessments [19]

Algorithmic Accountability and Impact Assessments seem popular in the United States (US) where many bills have been introduced to authorise the Federal Trade Commission (FTC) to make an assessment on whether corporate automated decision systems (ADS) products are biased, discriminatory or has privacy issues that would be detrimental to consumers.

Algorithmic Impact Assessments (AIAs) ensures that AI vendors and their customers have assessed and understood the social implications of their technologies before they are rolled out to be used by the public. These assessments would be published publicly so that the public can comment on them. It ensures that the AI system is safe for deployment and attaches as sense of responsibility to those who make and use them.[20]

If the Australian Government proposes to deploy an AI-informed decision-making system, it would be useful to engage in Algorithmic Accountability and Impact Assessments and enable it to ‘undertake a cost-benefit analysis of the use of AI, with specific reference to the protection of human rights and ensuring accountability, engage in public consultation, focusing on those most likely to be affected and only proceed with deploying this system, if it is expressly provided for by law and there are adequate human rights protections in place.’[21]

In the Australian context, the ACCC, OAIC and the Human Rights Commission should be able to work together in making these Impact assessments. As such, any standards relating to AI-informed decision making should include an assessment on human rights compliance.[22]

In line with the workings of the AIAs, the AI system should not be deployed in any context where decisions could infringe the human rights of individuals, [23] and the legal person who

[17] See proposal 7

[18] See Question B

[19] relevant to proposals 6, 8, 10, 12, 14, 15 and 18

[20] Reisman et al., ‘Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability,’ https://ainowinstitute.org/aiareport2018.pdf

[21] See proposal 6

[22] See proposal 12

[23] See proposal 8

deploys an AI-informed decision-making system should be legally responsible for the use of the system[24].

The nature of the AIA seems well suited for being used as a human rights impact assessment tool for AI-informed decision making and the making of a 'toolkit for ethical AI'.[25] It could also incorporate a regulatory sandbox to assess AI-informed decision-making systems to ensure compliance with human rights. [26] It should also ensure that any governmental procurement of AI systems would include adequate human rights protections. [27]

Biometric Recognition Regulation[28]

There is much privacy concerns on the use of biometric recognition and a national face database. Hence, the Australian Government should maintain a legal moratorium on the use of facial recognition technology until a legal framework with robust protections for human rights has been established. The legal framework should be developed in consultation with expert bodies including the Australian Human Rights Commission and the Office of the Australian Information Commissioner (OAIC). In addition, even if there was a legal framework, there should be certain situations which warrants the total ban of biometric recognition. For example, in looking at the European experience, it is noted that the data protection authority in France (CNIL) declared that the use of facial recognition in schools are illegal due to privacy concerns.[29] Similarly, such forms of facial recognition should be prohibited in Australia.

Algorithmic Transparency[30]

Algorithmic transparency ensures that the defendant in a court case has a right to access information about the technology that has been used by law enforcement agencies. There may be intellectual property rights attached to the proprietary technology which belongs to a private company, and these technologies may have been used by law enforcement agencies. In order for algorithmic transparency to occur, the defendant should be able to access information about the technology used by the law enforcement agencies despite the fact that it may have been protect by intellectual property rights. For example, the Justice in Forensic Algorithms Act 2019 is a US legislation that prohibits companies from preventing a defendant in criminal proceedings from obtaining information about their technical systems such as its source code. These companies would not be able to prevent the disclosures on their technical systems to the defendant in criminal proceedings on the grounds of protection of trade secrets, etc

[24] See proposal 10
[25] See proposal 14
[26] See proposal 15
[27] See proposal 18
[28] relevant to proposal 11
[29] 'CNIL Bans High School's Facial-Recognition Programs,' *IAPP*, October 29, 2019. https://iapp.org/news/a/cnil-bans-high-school-facial-recognition-programs/
[30] Relevant to Question C

Australia should enact legislation that is similar to the Forensic Algorithms Act 2019 in the US. Furthermore, Intellectual Property laws in Australia may need to be reformed to ensure algorithmic transparency if there are any provisions in the current laws that impedes it.

Task Forces or Commissions[31]

Task Forces are temporary quasi-government bodies which include external experts and government workers. They examine emerging technologies and publish their findings, and make recommendations on how the Automated Decision Systems (ADS) should be held accountable. This method has been implemented in several jurisdictions in the US, such as New York City, Alabama and Vermont.

The discussion paper's proposal[32] to establish a Task Force seems to align with this model. In addition, this Task Force may be used to conduct a 'comprehensive review, overseen by a new or existing body, in order to identify the use of AI in decision making by the Australian Government, undertake a cost-benefit analysis of the use of AI, with specific reference to the protection of human rights and ensuring accountability, outline the process by which the Australian Government decides to adopt a decision-making system that uses AI, including any human rights impact assessments, identify whether and how those impacted by a decision are informed of the use of AI in that decision-making process, including by engaging in public consultation that focuses on those most likely to be affected; and examine any monitoring and evaluation frameworks for the use of AI in decision-making'.[33]

Furthermore, much can be learned from the recent experiences of the Task Force in New York City (NYC).The workings of the NYC's ADS Task Force revealed some shortcomings which should be avoided by other Task Forces. Indeed, it was stated that future Task Forces in Alabama and Vermont should note the shortcomings in the NYC's taskforce to ensure that such shortcomings are not repeated.[34] The shortcomings in the NYC's Task Force are such as the lack of public engagement, the lack of consensus within the Task Force in the NYC's ADS Task Force's report which resulted in a biased report, as well as some omissions in the report'.[35]

Should Australia wish to establish a Task Force, it would be useful to glean from the lessons learned from the process undertaken by the NYC Task Force, as well as two recommendations for other jurisdictions which have been reported in 'Confronting black boxes: A Shadow report of the New York City Automated Decision System Task Force.' [36]

[31] relevant to proposals 13 and 17

[32] See proposal 13

[33] See proposal 17

[34] AINOW 2019 Report, December 2019, https://ainowinstitute.org/AI_Now_2019_Report.pdf

[35] AINOW 2019 Report, December 2019, https://ainowinstitute.org/AI_Now_2019_Report.pdf

[36] 'Confronting black boxes: A Shadow report of the New York City Automated Decision System Task Force.' https://ainowinstitute.org/ads-shadowreport-2019.pdf