Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D19/269

15 March 2019

Human Rights and Technology Project Team
Australian Human Rights Commission

By email only: tech@humanrights.gov.au

Dear Human Rights and Technology Project Team

Submission in response to the *Artificial Intelligence: governance and leadership* White paper

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission in response to the Australian Human Rights Commission (**AHRC**) and the World Economic Forum's White paper on *Artificial Intelligence: governance and leadership* (**the White paper**).

OVIC is the primary regulator for information privacy, data protection, and freedom of information in Victoria, and regulates the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982* (Vic).

Given the challenges, opportunities and implications of artificial intelligence (**AI**) for information privacy, I have a strong interest in the area of AI and its impact on privacy. In June 2018, my office published an *Artificial intelligence and privacy issues paper* (**AI paper**) exploring some of the issues relevant to AI and information privacy.[1] In October 2018, OVIC made a submission to the AHRC in relation to its *Human Rights and Technology Issues Paper*.[2] AI continues to be a key focus area in OVIC's current and future work.

One such issue identified in OVIC's AI paper relates to the governance of AI, the topic of the White paper and this submission.[3] As noted in OVIC's AI paper, government 'has a significant role to play in shaping how AI technologies impact citizens' lives through regulation, policy, and demonstrating best practices', for example by promoting human rights in the design, development, and deployment of AI technologies and systems.[4]

However, the establishment of any entity to govern or regulate AI, whether in the form of a 'Responsible Innovation Organisation' as proposed in the White paper or another model of governance, must take the broader regulatory network into consideration. This is particularly pertinent given the likely overlap with other regulators at both the state and federal level.

In addition to AI governance, this submission also briefly touches on issues of bias and consent in the context of AI, and the need for government to proactively protect and promote human rights.

---

[1] Available on the OVIC website at https://ovic.vic.gov.au/privacy/for-agencies/guidance-and-resources/research-papers/.
[2] See OVIC's *Submission in response to the Human Rights and Technology issues paper*, 2 October 2018, available at https://ovic.vic.gov.au/privacy/submissions-and-reports/submissions/.
[3] See page 13 of the *Artificial intelligence and privacy issues paper*.
[4] Ibid, page 6.

Interplay between different regulatory bodies

1. In recent years, there have been substantial developments in Australia's regulatory landscape in relation to public sector data reform and the management of personal information. Notably, these developments include the introduction of the Consumer Data Right (**CDR**); new data sharing and release reforms, with the establishment of the Office of the National Data Commissioner; and the Australian Competition and Consumer Commission's (**ACCC**) inquiry into digital platforms, part of which focuses on digital platforms' handling of consumer data and the role of privacy legislation in this context.[5]

2. As individuals become increasingly aware of the need to secure their information in today's digital economy, it is essential that these significant public sector reforms are delivered in a privacy-enhancing way that align with community expectations. Existing state and federal regulators will continue to play a crucial role in protecting and enforcing information privacy rights, including those that have not previously had an express role in regulating information privacy. The ACCC, for example, is proposed to be a co-regulator in the administration of the CDR scheme, along with the Office of the Australian Information Commissioner and a new Data Standards Body (the role of which is currently performed by Data 61).[6]

3. As the adoption of AI in the public and other sectors becomes more widespread, consumer data and personal information that falls under the remit of existing regulators may also potentially be covered by standards, regulation or legislation of an AI regulatory body. Such an entity will therefore be situated within, and intersect with, a broader regulatory network that encompasses different regulators for different types of data.

4. Given the potential interplay between other authorities that regulate data, it is appropriate that the role, functions, powers and jurisdiction of an AI governance or regulatory body are clearly outlined, to prevent ambiguity around regulatory enforcement action and avenues for redress — especially if, for example, a co-regulatory approach is adopted.

A mechanism for addressing state concerns

5. From a Victorian perspective, as AI becomes more prevalent across the public (and private) sector, the potential for Victorians' personal information to be involved in AI processes of organisations outside of Victoria (for example, other state or Commonwealth public entities) will likely grow. In such instances, the jurisdiction of state regulators such as OVIC needs to be made clear not only by law, but also operationally, to both other regulatory bodies and members of the public.

6. It is essential that individuals know where to make a privacy complaint or make enquiries about their personal information in a complex regulatory environment. For example, where a Victorian public sector organisation transfers an individual's personal information to another entity subject to the Commonwealth *Privacy Act 1988*, and that information is subsequently involved in AI processes, individuals' complaint rights and avenues for redress need to be clear to ensure individuals are best placed to exercise their information rights.

---

[5] See the ACCC's Digital Platforms Inquiry Preliminary report, December 2018, available at https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/preliminary-report.

[6] See The Treasury, Consumer Data Right Booklet, 9 May 2018, available at: https://static.treasury.gov.au/uploads/sites/1/2018/05/t286983_consumer-data-right-booklet.pdf.

7. A crucial part of OVIC's role as a state regulator is the proactive protection of Victorians' information rights in multi-jurisdictional environments, particularly given the number of recent reforms at the Commonwealth level involving consumer data.[7] This is in line with expectations of the Victorian public and OVIC's stakeholders. Collaboration between an AI regulatory body and privacy regulators in Australia can help achieve better informed policy outcomes and maintain public trust and confidence in the ability of privacy regulators in Australia to protect individuals' privacy, in their respective jurisdictions.

Understanding bias and the limitations of regulation

8. The White paper recognises the potential for creating 'a common benchmark for the design and deployment of AI systems across Australia'.[8] However, there are several factors that could complicate the development of these benchmarks. Bias, for example, is recognised as a key issue in the development of AI, one that has potentially unintended consequences — yet to date, there is no singular baseline or set of standards to evaluate bias. Bias can be present or created not only in the collection and preparation of the data used as input, but also in the design of a program's objectives.

9. Some of the issues relevant to the development of benchmarks are outlined below.

    - Algorithmic 'fairness' is not simply mathematically calculated – it is also socially determined. Many proposed quantitative measures of fairness are based on implicit assumptions about fairness in society.[9] Further, concepts of fairness are varied and contextual; what is considered to be fair in one context or by a particular group within society may not be in another context or by another group. While challenging, settling on a common framework for social fairness will be a necessary predicate for any benchmarking exercise.

    - Although methodologies for auditing influence in data models are becoming available,[10] there are limitations to their applicability.

    - Research from the United States indicates that there may be a 'portability trap' limiting the re-use of AI across different social contexts. This has repercussions for government, in particular, if AI is not based on data from broadly representative social samples, as models developed based purely on one social group will most likely not be applicable to other groups.[11]

    - Removing bias after it has been introduced during the development of a model is very difficult. This may pose challenges for organisations and governments that find themselves with models that accidentally (or by design) are discriminatory or unfair.[12]

---

[7] Section 8C(1)(f) of the PDP Act provides that one of my information privacy functions is to 'make statements in relation to any matter affecting personal privacy or the privacy of any class of individual.'

[8] See page 13.

[9] See Friedler, Scheidegger and Venkatasubramanian, 2016, *On the (im)possibility of fairness*, available at https://arxiv.org/pdf/1609.07236.pdf.

[10] For example, see Adler et al., *Auditing Black-box Models for Indirect Influence*, 2016, available at https://arxiv.org/pdf/1602.07043.pdf.

[11] See Selbst et al., *Fairness and Abstraction in Sociotechnical Systems*, ACM FAT* '19 *Proceedings of the Conference on Fairness, Accountability, and Transparency*, Atlanta GA USA January 2019, available at https://fatconference.org/2019/acceptedpapers.html.

[12] For example, see Amazon.com and its recruiting algorithm, which was shown to have introduced bias against women because it relied on implicitly gendered words. The company was forced to scrap the tool entirely because while the offending words could be removed there was no way to guarantee that the model would not include other unforeseen factors, as it relied on historical data. See https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

10. Accordingly, to be effective, any regulatory model developed to limit bias in AI will need to be accompanied by resources to investigate project assumptions, original data sources, model development, and model application. However, it is arguable whether bias-free AI can ever be developed; bias may still emerge even where 'reasonable measures' are in place to address the risk of it occurring. As such, consideration will need to be given to the possibility that where bias is identified, investment in an AI system may need to be written off. The unsuccessful deployment of AI (due to bias or another cause) can present a significant political challenge for organisations and governments alike, particularly if investment in the system has been significant.

Informed consent in the context of AI

11. The challenges of the traditional notice and consent model, and its limitations in protecting individuals' information privacy in today's digital and information economy, are concerns that OVIC has raised previously.[13] The limitations of consent are further intensified in the context of AI, where the complexity of the development, deployment and operation of AI (for example, machine learning techniques underpinning it) means that many, if not most, individuals lack the requisite knowledge to provide informed consent. If individuals do not have an adequate understanding of how their personal information will be used by an AI application or algorithm, their ability to exercise choices about their personal information is diminished.

12. However, the limitations of the traditional consent model are not solely due to individuals' ability to provide meaningful consent. The dynamic nature of AI and its ability to extract meaning from data means that, in many cases, developers and organisations using AI themselves do not – or indeed, cannot – know the extent of how AI will use personal information at the time it is collected. For example, personal information may be collected for a particular purpose, but with the advancement of technology or amalgamation of other data sets (which may not yet be in the organisation's possession or may not yet even exist), that information could then be used for purposes beyond those for which it was initially collected.

13. Further, the nature of AI and AI algorithms often mean that it can be a struggle for those developing and using AI to understand how a process has led to a particular outcome.[14] This makes it difficult for organisations to obtain meaningful consent if they cannot communicate AI processes to individuals. The challenges for organisations in understanding AI processes, and how AI could potentially use personal information in the future, mean that the traditional model of consent underpinning many privacy laws will be difficult to extend to an AI context.

14. While education can serve to improve individuals' knowledge of AI and enhance (to an extent) their ability to provide meaningful consent, this places the onus on the individual to be informed in order to protect their own privacy. It should be incumbent upon government to protect human rights, rather than placing the onus on the individual to do so for themselves.

15. As such, any new AI regulatory body, and any standards, regulation or legislation arising from the establishment of one, should address consumer protection in a proactive manner by setting baseline protections for consumers, rather than being merely reactive in receiving and adjudicating complaints. This may involve, for example, the body assessing AI algorithms and developing standards around those algorithms so that they are used in a way that is compatible with human rights, as a default requirement.

---

[13] See, for example, OVIC's *Submission in response to the Digital Platforms Inquiry preliminary report*, 15 February 2019, available at https://ovic.vic.gov.au/privacy/submissions-and-reports/submissions/.

[14] See page 8 of the *Artificial intelligence and privacy issues paper*.

Thank you for the opportunity to comment on the White paper. OVIC will continue to follow the progress of the AHRC's Human Rights and Technology project with interest, and I look forward to reading the AHRC's Discussion Paper later this year.

I have no objection to this submission being published by the AHRC without further reference to me. I also propose to publish a copy of this submission on the OVIC website but would be happy to adjust the timing of this to allow the AHRC to collate and publish submissions proactively.

If you have any questions about this submission, please contact Emily Arians, Senior Policy Officer at emily.arians@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner