Australian Government

Office of the Australian Information Commissioner

Human Rights & Technology Discussion Paper

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

6 July 2020

OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make this submission to the Australian Human Rights Commission's (AHRC) discussion paper, Human Rights and Technology (the discussion paper). The discussion paper provides a very insightful and thorough consideration of important issues facing Australia regarding the use of technology and its impacts. The discussion paper raises several important privacy issues, and comes at a time where reform to Australia's privacy framework is being considered, following the Australian Government's announcement of a review of the *Privacy Act 1988* (the Privacy Act).[1]

2. The OAIC has previously made submissions in response to the AHRC's Human Rights and Technology Issues Paper[2] and Artificial Intelligence: Governance and Leadership white paper.[3]

3. The discussion paper highlights some of the risks posed to human rights by new technologies, in particular, artificial intelligence (AI). AI technologies are increasingly being used by private and public entities. This has the potential to generate significant opportunities and efficiencies for business, government and the community. However, the use of these technologies also creates risks, including to privacy and other human rights.

4. Appropriate regulatory safeguards are necessary to realise the benefits and manage the risks that new technologies such as AI bring, and to give entities clarity about how to use these technologies in a way that adequately protects the rights of individuals. As these technologies commonly rely on significant quantities of personal information, we consider data protection is a central pillar of this regulatory approach which provides a framework for addressing many issues highlighted in the discussion paper. The upcoming review of the Privacy Act provides an opportunity to ensure it provides safeguards appropriate for the digital age.

5. The Privacy Act and the Australian Privacy Principles (APPs) address some of these risks, for example through requirements to have practices, procedures and systems in place to ensure compliance with the APPs, notice and consent requirements, and obligations to take reasonable steps to ensure the accuracy and quality of personal information.

6. However, the OAIC's view is that Australia's privacy framework requires reform to remain fit for purpose in the digital age. The OAIC is drawing on its regulatory experience, understanding of international data protection regimes, engaging with experts, regulated entities and the community in order to advise Government in the upcoming review.[4] This submission provides our current perspective on how enhancing the existing privacy regime would assist to address the risks created or magnified by new and emerging technologies, while avoiding fragmentation in the regulation of these tools. We offer observations about:

---

[1] https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/response-digital-platforms-inquiry

[2] https://www.oaic.gov.au/engage-with-us/submissions/human-rights-and-technology-issues-paper-submission-to-the-australian-human-rights-commission/

[3] https://www.oaic.gov.au/engage-with-us/submissions/artificial-intelligence-governance-and-leadership-white-paper-submission-to-the-australian-human-rights-commission/

[4] Section 28B of the Privacy Act sets out the Information Commissioner's advice related functions, which includes providing recommendations to the Minister regarding the need for legislative or administration action in the interest of the privacy of individuals.

- Modernising Australia's privacy framework
- Supporting privacy self-management through increased transparency
- Strengthening organisational accountability measures
- The uses of facial recognition
- The proposal for an AI Safety Commissioner.

Modernising Australia's privacy framework

7. Evolving technologies such as AI effect many areas of society and may have both positive and negative impacts. This also creates regulatory challenges, however, as these technologies are subject to several different legal frameworks. We consider this means that certain factors become more important to ensure effective regulation that enables innovation while protecting the community:
    - A co-ordinated, harmonised approach to law reform that avoids fragmentation of regulations amongst different regimes, to the extent appropriate.
    - Appropriate information sharing and co-operation between regulators, particularly in relation to AI.[5]
8. A National Strategy on New and Emerging Technologies, as set out in Proposal 1 of the discussion paper, may be an effective way of achieving these aims. This could be a standalone strategy or augment existing strategies such as those situated within the Department of Industry, Science, Energy and Resources, which has carriage of several other related strategies and roadmaps.[6]
9. The discussion paper comes at a critical point in the evolution of privacy protections in Australia, building on the Australian Government's commitment to reviewing the Privacy Act in its response to the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry Final Report.[7]
10. As part of the review, the OAIC considers that there is scope to strengthen and enhance mechanisms in the Privacy Act to address a number of the issues highlighted in the discussion paper that flow from the use of data in new and emerging technologies. These include reviewing the notice and consent model in Australia's privacy framework, the recourse available to an individual whose privacy has been breached by the use of AI technologies, and the challenges to effective redress that may be caused by the cross-border flows of personal information.

[5] For example, the OAIC, the AHRC, the Office of the National Data Commissioner, the eSafety Commissioner, the Australian Communications and Media Authority, the Australian Competition and Consumer Commission, and the Australian Securities and Investments Commission.

[6] See for example the Australia's Tech Future strategy, the National Blockchain Roadmap and Data Strategy 2018-2020.

[7] The Treasury, Government Response and Implementation Roadmap for the Digital Platforms Inquiry, 12 December 2019.

11. Based on the OAIC's regulatory experience,[8] there are four key areas of focus for reforms to ensure that the Privacy Act remains fit for purpose in the digital age:

    - Global interoperability — Making sure Australian laws continue to connect around the world, so personal information is protected wherever it flows.
    - Enabling privacy self-management — So individuals can exercise meaningful choice and control.
    - Organisational accountability — Ensuring there are sufficient obligations built into the system.
    - A contemporary approach to regulation — Having the right tools to regulate in line with community expectations.

12. The OAIC's perspective on the role of privacy self-management and organisational accountability in relation to AI technologies and automated decision making are explored further below. We seek to promote global interoperability by drawing on international best practice, minimising regulatory friction where that fits within the domestic context while looking to provide new solutions that suit Australia's unique needs.

Supporting privacy self-management

13. The OAIC supports the discussion paper's strong focus on transparency, which is a central theme in the Privacy Act. Transparency promotes privacy self-management by requiring entities to explain to individuals how their personal information is being handled.

14. This is particularly important with respect to AI technologies because those tools often use personal information as the basis for a decision that could have significant effects for the individual, but do so in a way that is often invisible or difficult to comprehend.

15. The discussion paper's proposal to enhance notice and transparency requirements are broadly consistent with proposed reforms to notice and consent in the Privacy Act that are currently being considered as part of the review of Australia's privacy framework.[9]

16. Accordingly, the OAIC suggests that notice and transparency requirements relating to automated decision-making are addressed by building on the foundations of the Privacy Act. This will avoid fragmentation and reduce complexity for individuals and regulated entities by setting out relevant notice obligations in a single regulatory regime.

17. The OAIC is considering the features of appropriate notice obligations in relation to automated decision-making and AI, drawing on work done by other regulators including the United Kingdom's

[8] This includes international experience and engagement in a range of international privacy and data protection forums, including cross-border regulatory matters. The OAIC is a member of the Global Privacy Assembly (GPA) and the Australian Information Commissioner is a member of the Executive Committee of the GPA.

[9] The Treasury, Government Response and Implementation Roadmap for the Digital Platforms Inquiry, 12 December 2019.

Information Commissioner[10] and the Office of the Victorian Information Commissioner.[11] We have two observations on the AHRC's proposed approach:

- In relation to Question A of the discussion paper, there are several important factors to consider when determining a threshold for enhanced notification rights regarding automated decision-making. The discussion paper proposes AI-informed decision-making as the threshold, which appears to be a positive adaptation of the threshold in article 22 of the GDPR. We note, however, that this may be considered in the review of the Privacy Act.
- In relation to Proposal 7 of the discussion paper, we agree that the provision of an explanation is important. Requiring entities to provide more technical information as part of their notification obligations could provide a basis for individuals (all be it with expert assistance where required) to contest decisions. Consideration will also be required on how such an obligation will address issues of commercial confidence. For example, the Privacy Act currently provides an exception to entities where an individual requests access to their personal information, and its provision would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Strengthening organisational accountability

18. The OAIC supports the discussion paper's three key principles on the design, development and use of AI in decision-making. These principles aim to ensure that the AI is used accountably, in a way that observes international human rights including privacy, while minimising harm to individuals. As the AHRC observes, building trust in AI technologies includes community confidence that Australia's regulatory framework will protect them from harm.

19. A key element of the OAIC's approach for proposed enhancements of the Privacy Act is to support transparency measures that promote privacy self-management by building in sufficient obligations into the privacy framework to hold organisations accountable for their information handling activities. This is also a central consideration for the international data protection community.

20. Striking an appropriate balance between privacy self-management and organisational accountability is particularly important for AI tools that may be difficult for individuals to understand and that may amplify existing privacy risks. The OAIC therefore supports Proposal 4 of the discussion paper which seeks to promote the lawful use of these tools by introducing a statutory cause of action for serious invasion of privacy. [12] This should be supported by legislative powers for the OAIC to appear or intervene in proceedings in appropriate circumstances.[13]

---

[10] For example, the 'Explaining decisions made with AI' guidance by the Information Commissioner's Office and The Alan Turing Institute.

[11] For example, the 'Closer to the Machine: AI e-book'

[12] This Proposal complements recommendations made in the recent ACCC Final Report on its Digital Platforms Inquiry and is consistent with international privacy regulatory developments in New Zealand, the United Kingdom, the United States and Canada.

[13] Office of the Australian Information Commissioner, *Digital Platforms Inquiry final report — submission to the Australian Government*

21. In addition, the OAIC's approach to enhancing organisational accountability requirements in the Privacy Act, outlined below, is aligned with the three key principles in the discussion paper to promote organisational accountability and protect individuals in the digital age:

    - **Creating additional privacy rights to protect individuals** – The OAIC considers that the review of the Privacy Act should ensure that it appropriately addresses emerging privacy harms in the digital age. This requires considering how the existing principles-based framework can be supplemented by additional individual privacy rights. These could include rights for an individual to request erasure of personal information, to object to the handling of their personal information or constraints on certain types of data processing that are contrary to user expectations in relation to privacy by establishing 'no-go zones'.[14] Other options include creating overarching enforceable rights, for example for regulated entities to ensure that all handling of personal information must be conducted fairly or lawfully, or introducing a statutory duty of care on entities to protect individuals from privacy harms.

    - **Mandating privacy by default and design –** The discussion paper highlights the importance of embedding strong safeguards in automated decision-making tools prior to deployment. A key aspect of promoting organisational accountability is privacy by design, which requires embedding privacy safeguards into the design of technologies, architecture and systems from their inception. Equally important is mandating that privacy settings are set pro-consumer by default.

    - **Promoting provable accountability –** Requiring regulated entities to demonstrate accountability will provide individuals with evidence-based information about the privacy credentials of entities with which they may engage. In addition to existing transparency measures in the Privacy Act, the OAIC has previously recommended other reforms such as introducing a third-party certification scheme,[15] and requirements for all APP entities to conduct a privacy impact assessment (PIA) for all projects designated 'high privacy risk'.[16] The OAIC suggests that any proposals regarding Human Rights Impact Assessments can draw upon and complement existing PIA requirements.

22. While general enhancements to the existing privacy framework could address several privacy risks highlighted in the discussion paper, a specific protection in relation to automated decision-making

[14] The Office of the Privacy Commissioner of Canada (OPC) has recognised inappropriate data practices, otherwise known as 'no-go zones'. Examples of 'no-go zones' that may be relevant to AI-informed decision making include profiling or categorisation that leads to unfair, unethical or discriminatory treatment contrary to human rights law, and collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual and surveillance by an organization through audio or video functionality of the individual's own device. Even with consent these practices are considered to be 'offside' for the purposes of Canadian privacy law. A no-go zone can be designated according to specified criteria, for example the sensitivity of the personal information, the nature of the proposed use or disclosure of that information, or the vulnerability of the individuals whose personal information is being processed.

[15] Australia is currently in the process of implementing the Cross-Border Privacy Rules (CBPR), which will provide a mechanism for governments and businesses to safeguard the free flow of data while protecting the privacy rights of individuals. The CBPR requires participating businesses to demonstrate compliance with a commonly understood set of privacy standards, establishing a level of certainty and assurance for the individuals providing their data.

[16] The OAIC recommended this in the Digital Platforms Inquiry Submission to the ACCC. This is already required by government agencies under the Privacy (Australian Government Agencies – Governance) APP Code 2017 for all high privacy risk' projects.

should also be considered. Such a protection already exists or is being considered in privacy frameworks in other jurisdictions.[17]

Government's use of AI-informed decision-making systems

23. Organisational accountability measures are particularly important for Government use of these technologies. We support Proposal 6 of the discussion paper, which highlights the significant value in ensuring transparency and accountability in Government AI-informed decision-making.

24. When considering the final recommendations to Government, we suggest the AHRC consider the interaction of Proposal 6 with the existing privacy framework. For example:

- The Australian Government Agencies Code requires Australian Government agencies to conduct a PIA for all high privacy risk' projects. The OAIC considers initiatives utilising AI technologies to process personal information are likely to be 'high privacy risk' projects. PIAs provide a useful framework for identifying the costs and benefits to privacy of AI-based systems.
- Several APPs provide an exception to the requirements of the APP for information handling that is required or authorised by an Australian law. For example, if required or authorised by law, entities may collect sensitive information without consent, or use or disclose personal information for a different purpose to the purpose for which it was collected. These exceptions create a framework that allow government agencies to carry out legislative functions without contravening certain privacy principles. We note, however, that several important privacy protections continue to apply (such as notice requirements and obligations to take reasonable steps to ensure the quality and security of personal information). These may be supplemented by additional organisational accountability measures if introduced as a result of the review of the Privacy Act.

Use of facial recognition

25. As highlighted by the discussion paper, there are several community concerns with widespread use of facial recognition technology. These concerns include risks to privacy rights. The use of biometric information and facial recognition technology is an area of regulatory focus for the OAIC.

Facial Recognition under the Privacy Act

26. Personal information that is used in facial recognition technologies and biometrics is regulated by the Privacy Act. Additionally, 'biometric information' and 'biometric templates' are classified as 'sensitive information', which is afforded a higher level of privacy protection than other personal

[17] See for example article 22 of Europe's General Data Protection Regulation (GDPR) and s71 of South Africa's Protection of Personal Information Act. A right modelled on the GDPR is also being considered in the United States of America which has looked to clarify this language from the GDPR. See for example Consumer Rights to Personal Data Processing Bill SF 2912 (Minnesota) (proposed legislation); New York Privacy Bill SB 5642 (New York) (proposed legislation); Protecting Consumer. Data Bill SB 5376 – 2019-20 (Washington State) (proposed legislation which is confined to profiling based on facial recognition). This right was also considered in a recent consultation paper on ensuring appropriate regulation of artificial intelligence by the Office of the Privacy Commissioner of Canada.

information. This recognises that inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual.

27. Unless an exception applies, entities must only collect sensitive information about an individual if the collection is reasonably necessary for (or for a Government agency, directly related to) one or more of its functions or activities and the individual consents to the collection. Exceptions include if the information is reasonably necessary for, or directly related to, an enforcement body's functions or activities, or if the collection is necessary for an entity to take appropriate action in relation to suspected unlawful activity or misconduct of a serious nature.

28. Similar exceptions apply to the use and disclosure of personal information for facial recognition. Personal information, including biometric information, can only be used or disclosed for the purpose of facial recognition if this is the primary purpose for collection or an exception applies. Relevant exceptions include if an individual has consented to this use or disclosure, if the use or disclosure is required or authorised by law, or if the entity reasonably believes that the use or disclosure is reasonably necessary for an enforcement related activity conducted by, or on behalf of, an enforcement body.

29. As with all personal information, the handling of biometric information is subject to other APPs including transparency obligations and requirements to ensure the accuracy and security of the information.

30. In the Government context, additional safeguards are in place to consider and mitigate against the impacts of facial recognition technologies. The Privacy (Australian Government Agencies – Governance) APP Code 2017 (the Australian Government Agencies Code)[18] requires agencies, including enforcement bodies, to undertake a PIA for all 'high privacy risk' projects. This can include projects that seek to use facial recognition technologies. This is a legislative requirement, and also gives agencies an important opportunity to engage with the community and explain why the proposed use is reasonable, necessary and proportionate to achieve a legitimate aim. A PIA can also identify the need to enact specific legislated safeguards in order to mitigate significant privacy risks.

OAIC's regulatory role

31. The OAIC's regulatory role includes handling complaints, conducting investigations, monitoring, advice and providing guidance on proposed uses of biometric information. We also conduct assessments of the handling of personal biometric information collected through and used in facial recognition technology.[19] The Information Commissioner may also make binding guidelines related to the use of biometric information and biometric templates.[20]

32. The OAIC is also monitoring developments related to the National Facial Biometric Matching Capability (NFBMC) and would have an oversight role of the Commonwealth's handling of personal information. The Parliamentary Joint Committee on Intelligence and Security (PJCIS) report on the

[18] Privacy (Australian Government Agencies – Governance) APP Code 2017 < https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/australian-government-agencies-privacy-code/>

[19] See, for example: https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-the-oaics-assessment-of-ibms-handling-of-personal-information-using-smartgate-systems/ and https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-the-oaics-assessment-of-department-of-immigration-and-border-protections-handling-of-personal-information-using-smartgate-systems/

[20] Section 28(b) Privacy Act and s 12(4)(c) of the *Australian Information Commissioner Act 2010*.

draft enabling legislation for the NFBMC has recommended the inclusion of a number of privacy protective measures to seek to ensure the proportionality of the identity matching services including:

- ensuring that appropriate privacy safeguards are set out in primary legislation and related policy documentation, such as:
  - requiring transparency and accountability for agencies involved in the collection and use of the personal information
  - requiring access controls to ensure that there are appropriate limitations around access to and use of personal information
- considering whether a warrant-based scheme for access should be implemented in relation to the use of 'one-to-many' identification technology[21]
- establishing appropriate regulatory oversight of the administration of technologies used to collect, use, and store biometric information, including:
  - proactive monitoring of appropriate use of facial recognition technology through regular, mandatory privacy assessments of the NFBMC, and
  - annual compliance audits of adherence to conditions set out in key agreement and policy documentation.

33. The consideration of the NFBMC by the JPCIS has brought to the fore community concerns about the large-scale deployment of facial recognition technologies. The JPCIS's recommendations for greater safeguards suggests that consideration should be given to commensurate legislative protections for any other uses of the technology that have a significant privacy impact.

Approach to law reform

34. The OAIC welcomes further consultation on the appropriate legal framework for the use of biometrics and facial recognition technology.

35. The review of the Privacy Act provides an opportunity to consider the regulation of facial recognition technology, taking account of the diverse contexts within which the technology may be employed, and the varying impacts on privacy. For example, reliance on consent for private sector uses of facial recognition technology poses risks if consent is not fully informed and freely given. In other contexts, individuals may choose to use biometric information for security and convenience.

36. The review of the Privacy Act can consider whether additional organisational accountability measures are required in relation to the use of facial recognition technology, including whether some uses are not acceptable to the community and should not be permitted. The OAIC will draw on its regulatory experience in the use of facial recognition technology, as well as research we have

[21] Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019*

commissioned into international approaches to regulation and oversight, to contribute to the review.

37. Alongside the review of the Privacy Act, all entities must ensure compliance with the Privacy Act when utilising facial recognition technologies. Given the potential impact on privacy, entities should take a careful and cautious approach to ensure they act transparently, lawfully and in accordance with community expectations. For Government, all proposed uses of facial recognition technologies should be reasonable, necessary and proportionate, informed by a PIA under the Australian Government Agencies Code for 'high privacy risk' projects. Where PIAs identify significant privacy risks, agencies should consider whether the project should continue or needs legislation in order to provide sufficient safeguards.

Establishing an AI Safety Commissioner

38. The OAIC supports increased co-ordination and co-operation within Government to develop appropriate policy and regulatory responses to AI technology.

39. In particular, we note that regulators require technical expertise to enforce regulatory schemes as the use of technologies such as AI becomes increasingly prevalent in the public and private sectors. Technical capacity-building within regulators would further support regulatory efforts. In addition or alternatively, a body could be established to act as a central source of technological expertise and capability to assist agencies and regulators to address these challenges. We consider that the UK Centre for Data Ethics and Innovation (CDEI), referred to in the discussion paper, is a model that has merit.

40. While we appreciate the challenges raised by AI, we query whether establishing a specialist additional independent commissioner is the most appropriate model. We suggest consideration is given to whether existing regulator bodies could be resourced to take on aspects, with legislated ability to share expertise and intelligence. An existing agency administering the proposed National Strategy on New and Emerging Technologies, potentially in collaboration with a technical body such as Data61, could also be an option for driving a whole-of-Government, economy wide approach to AI technology.