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: D18/134057

2 October 2018

Mr Edward Santow
Human Rights Commissioner
Australian Human Rights Commission
GPO Box 5218
SYDNEY NSW 2001

Dear Mr Santow

Submission in response to the Human Rights and Technology issues Paper

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission in response to the Australian Human Rights Commission's (**AHRC**) *Human Rights and Technology issues paper* (**the issues paper**).

OVIC is a regulatory body that has combined oversight of information privacy, data protection, and freedom of information in Victoria. As the Information Commissioner, I have a strong interest in matters that affect individuals' privacy, and one of my functions under the *Privacy and Data Protection Act 2014* (**PDP Act**) is to make public statements in relation to such matters.

The area of technology is of particular relevance to OVIC, as it often carries important privacy and security considerations. While we recognise that technology can enhance people's lives and create benefits for society as a whole, it can also challenge the principles and concepts underpinning information privacy.

In light of OVIC's remit, this submission focuses on the impact of technology on privacy as a human right. I have organised my comments in the attached submission around the consultation questions outlined in the issues paper. I have no objection to this submission being published by the AHRC without further reference to me. I also propose to publish a copy on the OVIC website.

Thank you for the opportunity to comment on the issues paper. I look forward to reading the AHRC's Final Report and recommendations for responsible innovation to protect human rights in Australia.

Yours sincerely

Sven Bluemmel
Information Commissioner

Office of the Victorian Information Commissioner

Submission to the Australian Human Rights Commission

The Office of the Victorian Information Commissioner (**OVIC**) is the primary regulator for privacy, data protection and freedom of information in Victoria, and administers the *Privacy and Data Protection Act 2014* (**PDP Act**). The PDP Act is the primary law in Victoria that protects the privacy of individuals' personal information held by Victorian public sector organisations, including government departments and agencies, universities, municipal councils, and statutory offices.[1]

Given this remit, this submission is focussed on the impact of technology on privacy as a human right. It is worthwhile to note that the PDP Act is limited to information privacy, which traditionally refers to an individual's ability to decide for themselves when, how, and for what purposes their personal information is collected, used and disclosed. However, there are other forms of privacy on which technology may also have a significant impact, including locational and territorial privacy. While this submission does not speak directly to these other facets of privacy, OVIC asks the AHRC to consider the impact of technology on the right to privacy more broadly.

Consultation questions

1. What types of technology raise human rights concerns? Which human rights are particularly implicated?

The impacts of technology on privacy are not new. However, the generation of exponentially increasing amounts of information (enabled, incidentally, by technological advances) mean that these impacts on information privacy are greater than ever before. For the private and public sector alike, protecting the right to privacy in this digital and information age is a growing priority. As more and more interactions people undertake are mediated by networks and machines, the appropriateness of a transaction-based model of information privacy should be questioned. Such a model depends greatly on an individual's understanding of technology in order to make informed choices (where possible) about their personal information.

While privacy is not an absolute right and must be balanced with other human rights, its importance should not be understated. The right to privacy is an enabling one, essential for the full enjoyment of other fundamental human rights such as the right to freedom of expression and freedom of association. The ability to exercise control over one's personal information – in other words, information privacy – is also essential to the development of one's identity and sense of self.

[1] The information privacy provisions of the PDP Act apply to those bodies listed in this paragraph; the protective data security provisions have a more limited application.

Many new and emerging technologies are shifting the privacy landscape significantly which, consequently, will have an impact on privacy rights. In particular, artificial intelligence (**AI**), surveillance, and Internet of Things (**IoT**) technologies present a challenge to the very principles and concepts underpinning information privacy legislation in Victoria, and around the world more broadly.

New technologies can pose an additional challenge for users. The context in which their information will be collected, used and disclosed needs to be transparent, which requires people to have a very well developed sense of the domain constraints of the app or device and any platforms it connects to. Given the complexities many modern and widely available types of technology present, for example IoT devices, it is increasingly difficult for individuals to develop a sophisticated understanding of the associated privacy impacts. Experience from several decades of enterprise IT suggests it is highly doubtful whether this challenge can be overcome with education or outreach.

Despite the challenges that they may pose to privacy rights, new and emerging technologies are not inherently incompatible with privacy. Rather, the extent to which individuals' privacy is enhanced or eroded depends on how the technology is designed and used. Identifying and implementing the right protections in the collection, use, and disclosure of personal information in any context (regardless of the type of technology involved, or if at all) is key to ensuring individuals' privacy rights are upheld.

Artificial intelligence

In June 2018, OVIC published an *Artificial intelligence and privacy issues paper*, which provides a high-level, non-technical overview of artificial intelligence (**AI**) and its implications, challenges, and opportunities for information privacy.[2]

One challenge identified in the paper is the blurring of the distinction between what is and is not considered personal information in an AI context. Many privacy laws around the world (including Victoria's PDP Act) are centred around the protection of personal information, which relies on the idea of identifiability – that is, whether or not a person's identity can be reasonably ascertained from a piece of information.[3] AI challenges this binary understanding of personal information in a number of ways, including through its ability to link and match data to individuals and to infer information from existing available data. In turn, determining what is and is not protected under privacy law according to the definition of personal information becomes increasingly difficult.

AI also challenges many of the core principles underpinning information privacy:

- The very nature of AI requires vast amounts of data in order to train and test algorithms. This may contravene the **collection limitation** principle, which is based on the idea of limiting the collection of personal information to only what is necessary for a particular function or activity.

- The **purpose specification** principle states that the purposes of collecting personal information should be specified to individuals. This is challenged by AI's ability to extract meaning from data beyond its original purpose of collection; as a result, organisations using AI technologies may not understand the potential for how the information ingested by AI can be used, thereby impacting their ability to provide genuine notice of collection to individuals, if the information is in fact used for secondary purposes.

---

[2] The *Artificial intelligence and privacy issues paper* can be accessed here.

[3] 'Personal information' is defined under the PDP Act as "information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion...".

- This in turn challenges the **use limitation** principle, as the potential for AI to reveal new and unforeseen uses of personal information, particularly in ways that may not be reasonably expected by individuals, is raised.[4]

- The transactional model of **consent** and privacy – that is, the idea that individuals are able to make choices about, for example, when and what personal information is collected, or how it is used – is increasingly and significantly challenged by AI. As AI uses personal information in exponentially novel or unexpected ways, a question that arises is whether individuals are truly able to exercise meaningful consent. Organisations that use AI technologies may themselves only have a rudimentary understanding of how the technology operates, resulting in their inability to convey this in any meaningful sense to individuals, who therefore have a limited ability to make an informed choice.

While these are certainly significant challenges to traditional notions of privacy, AI also has potential to enhance individuals' privacy rights – for example, by learning a person's privacy and consent preferences over time and applying those across a multitude of different platforms and services.

Surveillance technologies

Surveillance devices are another technology that raise privacy concerns, particularly as they become increasingly ubiquitous. There are many different types of surveillance technologies, from closed-circuit television (**CCTV**) and body worn cameras, to drones. Surveillance can also encompass the monitoring, interception, collection, and retention of communications.

Similar to AI, one of the privacy risks arising from surveillance technologies is the potential overcollection of personal information, where surveillance activities may collect more information than is necessary. Such activities may also be unreasonably intrusive and disproportionate to the purpose they are trying to achieve.

Another risk posed by surveillance is function or scope creep, where information collected by surveillance technologies is used for a purpose other than that for which it was originally collected. These examples are just some of the ways that surveillance technologies can impact on individuals' ability to exercise control over their personal information.

However, as noted above it is the way in which surveillance activities are designed, and how surveillance technologies are used, that will determine the privacy impacts of such technologies. The *Guidelines to surveillance and privacy in the Victorian public sector*, developed by the former Commissioner for Privacy and Data Protection, contain best practice principles for respecting individuals' right to privacy when deploying surveillance technologies.[5]

One of these principles is based around the notions of necessity, proportionality, and legitimacy – that surveillance use must be necessary and only collect the minimum amount of information required, proportionate to the problem being addressed, and for a legitimate purpose related to an organisation's functions or activities.

Internet of Things

The growing number of everyday devices and sensors with the ability to wirelessly connect to the internet and to each other presents another challenge to privacy. Known as the 'Internet of Things', these technologies can collect, generate, measure, and analyse large amounts of personal information.

[4] The PDP Act contains eight exceptions permitting the secondary use of personal information – see Information Privacy Principle 2 (Use and Disclosure).

[5] The *Guidelines to surveillance and privacy in the Victorian public sector* can be accessed here.

Along with the common privacy risks relating to the overcollection and secondary use of information as outlined above, there are additional challenges surrounding the transparency of IoT devices' collection of personal information. Often, these technologies operate in the background of people's everyday environment, without their knowledge or understanding that their personal information is being collected, or that new information is generated about them, such as information generated by fitness trackers during exercise, or home assistant devices. This has clear implications on information privacy rights – without knowing their information is being collected, used, or disclosed, individuals cannot exercise control over their personal information. The interfaces of IoT devices are often opaque to the user, providing no information on the actual transmission of data, or the security of the device.

Of particular concern when addressing the Internet of Things is that what may be considered good security today may be rendered inadequate security tomorrow, for example if a new exploit or vulnerability is uncovered or developed. For this reason, OVIC is of the view that proposals such as 'trust marks' or security scores are not appropriate. Unless devices can be dynamically updated (which is not easy given network complexity and consumer inattention) there is no persistent value for 'good' in terms of the security of IoT devices.

2. **Noting that particular groups within the Australian community can experience new technology differently, what are the key issues regarding new technologies for these groups of people (such as children and young people; older people; women and girls; LGBTI people; people of cultural and linguistically diverse backgrounds; Aboriginal and Torres Strait Islander peoples)?**

There is no one single definition or understanding of privacy; it encompasses many related but different concepts. Individuals (or groups of individuals) will value and experience privacy in varied ways. What is privacy enhancing to one individual or one group or culture may be privacy invasive to others.

This highlights the need for technologies to be designed with customisable preferences to cater for different perceptions of privacy. Providing the option to edit privacy settings at a granular level, rather than a default, one size fits all approach, may assist individuals to exercise control over their personal information, irrespective of how they may conceive of privacy or the value they place on being able to control their personal information. However as mentioned above, the volume of transactions, and the difficulty for most people in understanding the context and impact of transactions, means that effective design may not solve all problems. In the case of IoT devices, this information may not be available or may not be comprehensible.

Children and young people are another group that face different privacy challenges. This group is often considered more vulnerable than others to the misuse of their personal information, or improper data handling. However, children and young people are also early adopters and enthusiastic users of new technology, and indeed may be more at ease using them than are other groups.

When it comes to new technologies, protecting the privacy rights of children and young people is extremely important, especially as they mature and develop their identities and sense of self. An issue in relation to children and young people's privacy rights (and more broadly, those of the general public) is transparency. New technologies often involve the collection of large amounts of personal information and new uses for that information. It is often difficult for everyday individuals – let alone vulnerable groups such as children and young people – to understand what information is being collected and for what purposes, and how decisions about them are made. The need for organisations to be transparent in the way they deal with personal information, in a manner that is clear and understandable, is critical as technologies become increasingly integrated with our lives. Particular attention needs to be given to the needs of individuals from culturally and linguistically diverse backgrounds in this regard.

3. How should Australian law protect human rights in the development, use and application of new technologies?

In Victoria, the right to information privacy is protected by a web of legislation, including the PDP Act.[6] Victoria also has the *Charter of Human Rights and Responsibilities Act 2006* (**the Charter**), only one of two jurisdictions in Australia to have a charter of human rights.[7]

The right to privacy is enshrined in s 13 of the Charter, which requires public authorities, such as Victorian state and local government departments and agencies, to consider human rights (including the right to privacy) in decision making processes.[8] Victoria's legislative process also accounts for the right to privacy, with any new Bills introduced into Victorian Parliament required to be accompanied by a statement of compatibility against the Charter, assessing how the Bill aligns with human rights.

At a federal level, the Commonwealth *Privacy Act 1988* forms part of Australia's implementation of the right to privacy, as a signatory to the *International Covenant on Civil and Political Rights* (**ICCPR**). However, the absence of express statutory protections (as is the case in Victoria) at the Commonwealth level may limit the extent to which privacy as a broad concept can be upheld. Such statutory protections would ensure that decision makers consider a broader right to privacy in the development and uptake of new technologies, regardless of other approaches to regulation that Australia may adopt.

While a charter of human rights would offer a valuable mechanism for protecting the right to privacy, it is also important that other approaches to regulate the development, use, and application of new technologies similarly uphold individuals' human rights. Legislation that is principle-based, such as the PDP Act, is valuable in offering flexibility in how protections can be applied in varying contexts, and across evolving technologies and social norms. Given the fast pace of change in technology, principle-based legislation would be more effective compared to prescriptive legislative approaches, enabling protections to evolve as the technology does.

Notwithstanding the benefits of principle-based legislation, it also has its limitations, particularly in an environment where personal information has the potential to be used for purposes beyond what an individual may have consented to or may reasonably expect. In a world in which many people may not be aware of, understand or able to recall the permissions they gave a platform a few days earlier, it is increasingly difficult for an individual to make an effective risk-benefit analysis in relation to the information they provide the platform. An additional framework – or principles that implement minimum protections – around the development, use, and application of technologies and data would be valuable, in order to establish a baseline standard of privacy. This ensures that individuals' personal information is still protected even where they may not have a full understanding of the potential privacy implications.

In addition to core privacy principles underpinning legislation, regulation of new and emerging technologies should also encourage a Privacy by Design approach, which will help to protect the right to privacy by ensuring that privacy is considered and built in to the design, development, and implementation of technologies involving the collection and handling of personal information. A common way of applying Privacy by Design in practice is by conducting a privacy impact assessment (**PIA**). PIAs serve as an important tool for organisations to identify the privacy impacts of new projects and develop risk mitigation strategies, and in doing so, ensure that individuals' information privacy rights are considered and protected before any information is collected or used.

---

[6] For example, the *Health Records Act 2001* protects the privacy of health information. The privacy obligations of the Commonwealth *Privacy Act 1988* may also apply to some organisations.

[7] The Australian Capital Territory has enacted the *Human Rights Act 2004*.

[8] For more information refer to the Victorian Equal Opportunity and Human Rights Commission's website.

Regulation that promotes good privacy governance is another element for upholding information privacy rights. This involves taking proactive steps to promote and protect privacy, and encouraging accountability for information handling practices. The way that organisations manage their privacy governance can also enhance public trust and confidence, and importantly for governments, build social licence to collect and use people's personal information.

Additionally, procedural safeguards will help give effect to legislation in this area. This may involve, for example, establishing an external oversight body to ensure the effectiveness of legislation and hold organisations accountable. Our response to question 7 covers this in further detail.

4. **In addition to legislation, how should the Australian Government, the private sector and others protect and promote human rights in the development of new technology?**

While legislation forms an important part of a regulatory framework, other instruments should also be implemented in order to enliven the intent of legislation. This may include clear guidance on how to practically apply relevant principles, not only in the development of new technology, but also in its design, adoption, and use.

Human centred design is a useful technique to aid understanding of the interaction between people and technology. Experience in this field shows that people often act in different ways than intended by designers. Observation of people interacting with systems, attention to user feedback, and a willingness to use that feedback in iteration of the design of systems is at least as important to the privacy and security of those systems as regulation.

Aside from regulation, the right to privacy can be protected and promoted through incorporating stakeholder consultation in the process of developing new technologies, particularly those that involve personal information. Stakeholder engagement will also be crucial for promoting public acceptance and building a social licence for the use of new technologies that deal with personal information.

Stakeholder engagement should involve consultation with the individuals or groups whose information privacy rights will be directly impacted upon by the technology; this is particularly important for minority groups and vulnerable people, such as those noted in question 2 above. Such engagement should not be a once-off consultation that occurs only in the preliminary stages of the development of a new technology – effective stakeholder engagement requires a continuous process of information sharing and feedback from end users and regulators.

5. **How well are human rights protected and promoted in AI-informed decision making? In particular, what are some of the practical examples of how AI-informed decision making can protect or threaten human rights?**

AI-informed decision making can pose a substantial challenge to individuals' information privacy rights. As noted earlier, individuals risk losing control over their personal information, particularly in how their information may be collected and used to feed into the AI technologies and applications used in a decision making process. In some instances where the use of personal information in AI technologies may be unprecedented or unexpected, individuals may not even be aware that their personal information is being used to inform decision making.

This relates to another principle underpinning information privacy: openness. AI-informed decision making can challenge this where the logic or process of how a decision is made is unclear and difficult to communicate to individuals. This notion of transparency in information privacy (for example, knowing what information is collected, why, and how it is used) is crucial for individuals to be able to exercise meaningful control over their personal information.

The opaqueness of an AI-informed decision making process can also impact on organisations' ability to be transparent in their information management practices, which may be required by law. One of the IPPs under the PDP Act, for example, relates to openness and requires Victorian public sector organisations to have clearly expressed policies on how they manage personal information, including how it is collected and used.[9]

Conversely, AI-informed decision making also has the potential to protect information privacy rights. For example, AI algorithms that are able to explain how and why a decision was reached could be developed, and in this way facilitate transparency around how personal information is being used in a decision making process.

Protecting the right to privacy in AI-informed decision making processes will require proper oversight and good governance frameworks, which is addressed further in question 7 below.

6. How should Australian law protect human rights in respect of AI-informed decision making?

The uptake of AI technologies and capabilities in the public sector is steadily increasing in Victoria, and in Australia more broadly. The use of virtual assistants on public sector websites, for example, demonstrates that AI applications are fast becoming the norm, and will only become more integrated into individuals' lives and government processes.[10]

The emerging ubiquity of AI applications highlights the need for privacy-enhancing principles that guide the design, adoption, and use of AI-informed decision making, as well as other measures discussed above that will serve to protect information privacy rights (such as entrenching a Privacy by Design approach into program development).

Regulation in the area of AI-informed decision making should give particular focus to the principle of data quality, given that such a process relies on large amounts of data, which may include personal information. Inaccurate data can have a significant and potentially adverse impact on decision making, and consequently an individual's life.

Another significant objective of regulation should be to promote and enhance transparency and accountability in AI-informed decision making processes, particularly since such processes can be, by their very nature, opaque and difficult to understand or communicate. As aforementioned, transparency – specifically, algorithmic transparency – is essential for an individual's ability to exercise their information privacy rights, as well as for building trust and creating social licence.

While regulation around AI-informed decision making is still nascent, Australia can learn from international approaches towards protecting the right to privacy in this context. In particular, the European Union's General Data Protection Regulation (**GDPR**) offers enhanced privacy protections for individuals, and includes provisions specifically relating to automated decision making processes. The GDPR adopts a rights-focused approach, providing individuals with actionable rights and a clear pathway for redress outlined within the Regulation.

Article 13 of the GDPR, for example, provides that a data subject (an identified or identifiable natural person)[11] has the right to be made aware of the existence of automated decision making processes, and be provided meaningful information about the logic and envisaged consequences involved in such processes. Further, Article 22 of the GDPR also provides data subjects with the right not to be subject to a decision based solely on automated processing, except in certain situations.

---

[9] Information Privacy Principle 5.
[10] For example, see https://beta.ato.gov.au/Tests/Introducing-Alex--our-new-web-assistant.
[11] Article 4(1).

7. In addition to legislation, how should Australia protect human rights in AI-informed decision making?

As noted above, developing accompanying guidance on the principles to consider when undertaking AI-informed decision making can help bring the intent of legislation to life, assisting decision makers to implement processes in a way that is practical and protects the right to privacy.

Further to accompanying guidance, OVIC also supports the establishment of an independent body that regulates and promotes responsible innovation in AI-informed decision making. Although there will be an interplay of other regulators whose remits may overlap in this area (for example, privacy regulators will continue to have a role in protecting and enforcing information privacy rights), there is much value in having a regulator with the relevant technical expertise in the area of AI, which other regulators may lack. Good governance depends on a solid understanding of the technology used in AI-informed decision making.

In turn, governance plays an important role in protecting information privacy rights. It can be used to promote good design, implementation, and oversight of AI-informed decision making, and enshrine the right to information privacy within those processes.

However, regulators alone cannot achieve good privacy governance. It also requires a commitment on behalf of those designing, implementing, and using AI – as well as those controlling the information used in AI-informed decision making – to play a role in embedding privacy protections.

[Document ends]