information and privacy commission
new south wales

Enquiries: Sarah Wyatt
Telephone: 1800 472 679
Our reference: IPC20/A000015

24 February 2020

The Human Rights and Technology Team
Australian Human Rights Commisison

For submission via: https://tech.humanrights.gov.au/consultation

Dear Commissioner

HUMAN RIGHTS AND TECHNOLOGY DISCUSSION PAPER

This is a submission to the *Human Rights and Technology Discussion Paper* (December 2019) (Discussion Paper) prepared by the Australian Human Rights Commisison (the Commission). This submission provides general commentary and specific responses to identified proposals and questions contained within the Discussion Paper.

Introduction

New technologies, including artificial intelligence (AI) and the use of big data can be powerful tools for strengthening human rights. Increased access to social media tools, AI and data collection enable messages about human rights to be disseminated quickly and to broad audiences. Such technologies enable businesses and governments to better target their resources to benefit the community. However, emerging technologies, including AI, access to data and data security raise critical legal, regulatory and ethical questions for business and government requiring innovative responses.[1]

Rights oversighted by both the Information Commissioner and the Privacy Commissioner are frequently impacted by new and emerging technologies. Maintaining trust and confidence that rights will be preserved will ensure public acceptance in the utilisation of these technologies and contribute to informed decision-making by government. Under extant legislation enshrining these rights, modifications and exceptions operate, for example, public interest directions and privacy codes of practices under the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act). These provisions are directed to maintaining transparency and accountability in the handling of personal information. Similarly, provisions of the PPIP Act recognise that the operation of the *Government Information (Public Access) Act 2009* (GIPA), which enshrines the right to access government information are not affected by the PPIP Act.[2]

[1] Deloitte have recently explored issues arising from managing ethical complexities in respect of AI and data.

[2] PPIP Act, section 5

The Commissioners suggest a 'public interest test' provides a useful framework to ensure that where governments seek to employ new technologies it is for the common good, and existing information access and privacy rights and other human rights are maintained. The GIPA Act enshrines a public interest test and this enables the balancing of rights and interests.

Privacy and information access rights must be considered in the context of related considerations including cyber security, customer value and ethics in the context of new and emerging technologies. Where fundamental rights are modified by a proposed initiative or project that uses AI and new technologies, the reasons for the decision to modify those rights should be transparently explained.

PROPOSALS

Proposal 1: The Australian Government should develop a National Strategy on New and Emerging Technologies. This National Strategy should: (a) set the national aim of promoting responsible innovation and protecting human rights (b) prioritise and resource national leadership on artificial intelligence (AI) (c) promote effective regulation— this includes law, coregulation and self-regulation (d) resource education and training for government, industry and civil society.

We support the principle of effective and consistent regulation and also recognise the jurisdictional responsibilities of states and territories together with legislation and other regulatory tools that operate relative to new and emerging technologies. A national strategy on new and emerging technologies would demonstrate a national commitment to addressing what is a new and evolving aspect of the human condition. Just like the regulatory and legal challenges that arose in respect of industrialisation of previous centuries, governments of today need to address the emerging legal, regulatory and ethical issues that arise from use of emerging technologies, including AI.

We support the following three key regulatory principles identified in the discussion paper:

- Regulation should protect human rights and have regard to applicable laws
- Regulation should be clear and enforceable
- Effective co-regulation and self-regulation (through professional codes, design guidelines and impact assessments) can support regulation of new technologies.

Proposal 1(a) set the national aim of promoting responsible innovation and protecting human rights

As described, this object has ready application to all necessary functions to support responsible innovation and protect human rights including policies, standards and legislation.

A national strategy should recognise and acknowledge the benefits of new technologies and AI whilst ensuring their use in the public interest is subject to appropriate regulation and education of the government and community.

Inherent in this proposal is a need to effectively deal with the interaction of State, Territory and Commonwealth laws including soft law as they relate to information governance broadly and the establishment of rights including information access and privacy.

A mechanism to identify and evaluate extant legislative provisions together with regulatory tools that may be impacted by a national approach would provide a baseline from which to progress the proposal.

Information Commissioners throughout Australia have developed:

- A jurisdictional compendium that provides a comparison of information access legislation

- A framework of key features that are considered essential to the effective operation of information access legislation.

Proposal 1(c) promote effective regulation— this includes law, coregulation and self-regulation

Public Interest Test

In our view, the codification of a public interest test is an established and valuable decision making mechanism to inform determinations that impact rights. The public interest test is applied in both the information access and privacy jurisdictions.[3] Within these jurisdictions the public interest test applies a framework for independent decision making that mandates an objective which can only be displaced by other overriding considerations.

GIPA Act

Under the GIPA Act there is a general public interest in favour of the disclosure of government information. The GIPA Act provides for a balancing of considerations in favour of and against disclosure, having regard to the public interest. This is known as the 'public interest test'. The test requires consideration of:

1. The presumption in favour of release of government information;

2. Identification of factors in favour of disclosure;

3. Identification of factors against disclosure; and

4. Balancing of factors to determine where the public interest lies.

[3] Section 41(3) of the PPIP Act, for instance, provides that the Privacy Commissioner is not to make a direction exempting agencies from complying with principles and codes unless the Privacy Commissioner is satisfied that the public interest in requiring the public sector agency to comply with the principle or code is outweighed by the public interest in the Privacy Commissioner making the direction.

There is an overriding public interest against disclosure of government information if (and only if) there are public interest considerations against disclosure and, on balance, those considerations outweigh the public interest considerations in favour of disclosure. The balancing of public interest considerations may necessitate consideration of privacy protection principles and the interaction between the GIPA Act and the PPIP Act is well established within both statutes. The GIPA Act facilitates privacy protection through mechanisms including creation of a new record and redaction of information. Sections 5 and 20(5) of the PPIP Act recognise that the GIPA Act is not limited by the PPIP Act and therefore information may be released under the GIPA Act (either proactively or in response to an application).

The principles set out in section 15 of the GIPA Act guide the application of the public interest test. One principle recognised is that disclosure of information which might cause embarrassment to or loss of confidence in the Government is irrelevant and must not be taken into account. There is recognised value in applying principles to guide public interest decisions.

Application of the public interest test in the context of digital technologies and rights promotion

The European Union recommends a rights impact assessment in the development and delivery of AI.[4] Within the Australian legal context public interest tests are well established and are used to perform an assessment of rights impacted in a number of contexts.

The public interest test is an enabler in the protection and management of information. Legislation is an important tool for setting out rights and responsibilities. There is scope for a 'public interest test' to be utilised in the regulation of and facilitation (through legislation) of new technologies and AI by government.

There will be many interests that need to be balanced in respect of technology initiatives. These interests can include privacy, human rights, security, intellectual property, societal benefits and data monopolies to name a few. It is not clear how these diverse interests would be balanced unless the public interest is clearly defined.

Consideration of the public interest test has been seen in other contexts. For instance, in March 2019 the Commonwealth Government released *Best Practice Guide to Applying Data Sharing Principles*. This paper introduces an established concept – not of individual rights, but of collective rights of public benefit as a defining test. The purpose of the Guide is to assist agencies that hold Australian Government data (data custodians) to safely and effectively share the data they are responsible for by using five Data Sharing Principles. Where there is a clear public benefit, data custodians may seek to share data in a controlled manner with a range of users, such as Government agencies, the academic research community and, in some cases, the private sector.

[4] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

The public interest assessment contained in the Guide is not without constraints. The Guide also recognises that safeguards must be applied and that these safeguards must increase in proportion to the sensitivity of the data. In this way, existing legal rights and protections that benefit individuals and society must be acknowledged and respected with the ultimate assessment guided by the public benefit.

Contemporary public management approaches have introduced the concept of public value – the creation of a new right claimed by citizens to services they have authorised or funded through democratic processes.[5] In part, this approach responds to the recognised need to engage with citizens, to be representative and responsive to their needs.

Regulation in the digital age

The digital age has disturbed the traditional legal and regulatory environment. As one commentator recently wrote:

> *Conceptually, consent is an even less appropriate means to authorise data flows in the context of AI than in other contexts. Consent would likely be ineffective where AI is concerned; most people would be unaware of the impacts of AI or its possible consequences and as a result 'informed' and 'specific' consent would be near impossible to achieve.*[6]

Established consent requirements are even more challenged in a context where the ultimate use of data-informed technology may not be known. Data can be applied in an infinite number of ways to achieve an infinite number of outcomes. Some of these applications might not be within the contemplation of the custodian, but rather they are to be realised sometime in the future.

Proposal 2: The Australian Government should commission an appropriate independent body to inquire into ethical frameworks for new and emerging technologies to: (a) assess the efficacy of existing ethical frameworks in protecting and promoting human rights (b) identify opportunities to improve the operation of ethical frameworks, such as through consolidation or harmonisation of similar frameworks, and by giving special legal status to ethical frameworks that meet certain criteria.

This proposal suggests commissioning an independent body to assess the efficacy of existing ethical frameworks in protecting and promoting human rights and identify opportunities to improve the operation of ethical frameworks.

Ethical frameworks that consider the utility of the use case; the promotion of just outcomes; existing rights; public value; common good and harm minimisation have been developed to solve complex ethical problems. Those frameworks promote the balancing of these sometimes-competing interests to produce a transparent outcome that provides the accountability that citizens within democracies should legitimately expect.[7]

---

[5] Tom Frame (ed), *Who defines the Public Interest* (Connor Court Publishing Pty Ltd, 2018).

[6] https://www.salingerprivacy.com.au/2019/04/27/ai-ethics/.

[7] https://www.scu.edu/ethics-app/.

Internationally ethical frameworks have developed in the context of rapid developments in information technology, including AI. These frameworks provide a form of soft regulation and in general operate absent specific legislative/regulatory authority. However, human rights within the Australian context are enshrined in a number of statutes. A solely ethical approach to evaluating or regulating the impact of technology on human rights appears inconsistent with the legislative codification of human rights.

We support the establishment of an ethical framework for new and emerging technologies that recognises and reflects extant legislation. Consideration of existing ethical models is an important comparator and precedent with which development of a new framework may be undertaken. There may also be scope to consider consolidating existing frameworks, where appropriate.

Rapid technological innovation has generated the widespread application of AI in an array of contexts including government decision making. Government exercises a unique and significant role in the development and application of citizen rights. Accordingly, with rapid developments and the demonstrated utility of AI there is a pressing need for Government to lead an assessment of the efficacy of existing ethical frameworks in protecting and promoting human rights.

The NSW Information and Privacy Commission (IPC) is currently exploring provision of advice to NSW agencies and the Government through development of a public interest framework (PIF) and a digital audit tool.

The PIF recognises statute-based rights and provides an effective mechanism to ensure that rights are identified and preserved through informed decision making relevant to significant digital policy and projects. The PIF is supported by specified governance arrangements. This work has progressed to consultation within government. The development of an agency audit tool will complement the PIF and operate to guide the development of proposals from inception and ensure that they identify rights impacted by the proposal. Accordingly, the tool will provide a trigger to activate consultation with the IPC regarding the potential impact upon information access and privacy rights together with other relevant action. We anticipate progressing this work in 2020.

An innovative, robust and responsive solution is required to address the critical legal, regulatory and ethical questions faced by businesses and governments in dealing with new technologies. A framework that successfully builds upon existing rights and provides a clear methodology for balancing those rights within existing legal mechanisms for a public benefit, may provide that solution.

The efficacy of that solution is in part dependent upon a holistic approach. Currently jurisdictions within Australia and internationally operate according to a fractured model of information governance which may in many circumstances exacerbate potential tensions between rights relevant to information governance, for example, the right to privacy and the right to access information. This approach manifests in tools for application by government agencies responsible for information governance including privacy impact assessments and data protection impact assessments. While there is merit in the use of these tools, these approaches fail to provide a holistic solution to guide information governance by agencies and assist in balancing those rights where they conflict.

The Commission's Discussion Paper recognises the many rights that may be impacted by AI and this provides an opportunity to explore options for a holistic response.

There are a number of principles that should inform the independent review of the efficacy of existing ethical frameworks. In particular, regulatory principles have demonstrable application and utility.

Effective regulation recognises the principle of proportionality. Regulatory intervention must be informed by the potential or actual harm associated with the action or inaction under examination and be applied with a commensurate level of force to ensure a sustainable outcome.

In respect of new technologies and AI initiatives it is important that the following issues are explored and understood:

- How is government data managed, who uses it, and for what purposes?
- Does the initiative involve technological, algorithmic and artificial intelligence systems that impact citizens' lives?
- How does the initiative ensure the ability to question and change unfair, biased or discriminatory systems?
- How will access to digital services on equal terms be ensured?
- What is the impact on managing digital infrastructures and data as a common good?
- How does the proposal promote public interest objectives?
- How are digital service standards ensured and utilised?
- What skills/capability might be required of the public sector and citizens?

Understanding the above issues will ensure that privacy and information access rights are safeguarded, and initiatives are developed in the public interest. A recent example of such a framework (recognised in the Discussion Paper) is the *AI Ethics Framework in November 2019* prepared by the Australian Government Department of Industry, Innovation and Science.[8]

We agree with the Commission's observation that ethical frameworks 'can be important, but they cannot be a substitute for the law.'[9] We see value in ethical frameworks supplementing the law to lead to good decision making by government in the public interest. Such frameworks are flexible and responsive to changing needs and interests. In this regard, we we consider the European Commission's *Ethics guidelines for trustworthy AI* a useful model.[10] The guidelines suggest that trustworthy AI should be:

1. lawful - respecting all applicable laws and regulations

[8] Discussion paper, 49.

[9] Discussion paper, 55.

[10] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

2. ethical - respecting ethical principles and values

3. robust - both from a technical perspective, while taking into account its social environment.

Proposal 4: The Australian Government should introduce a statutory cause of action for serious invasion of privacy.

We consider that a national approach to this issue is required, rather than a fragmented, piecemeal approach to a privacy protection of this kind.

We support in-principle a statutory cause of action for serious invasions of privacy at the national level. We say this noting the cross-jurisdictional aspects of such invasions of privacy (for example online, interstate and internationally). We note the NSW Government separately expressed this view in its response to the 2016 report of the NSW Standing Committee on Law and Justice (referred to below).

Previous consideration of a statutory cause of action for serious invasions of privacy

The issue of remedies for serious invasions of privacy has been considered extensively at both the Commonwealth and state level over the past two decades. There have been multiple reports by law reform bodies and parliamentary committees examining the existing remedies for serious invasions of privacy and considering the possible features of a statutory cause of action, namely:

- 2008 Australian Law Reform Commission report, *For Your Information: Privacy Law and Practice, Report 108*
- 2009 NSW Law Reform Commission report, *Invasion of Privacy, Report 120*
- 2010 Victorian Law Reform Commission report, *Surveillance in Public Places, Report 18*
- 2011 Commonwealth Government Issues Paper, *A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy*
- 2014 Australian Law Reform Commission report, *Serious Invasions of Privacy in the Digital Era, Report 123*
- 2016 Senate Legal and Constitutional Affairs References Committee report, *Phenomenon colloquially referred to as 'revenge porn'*
- 2016 NSW Standing Committee on Law and Justice report, *Remedies for the Serious Invasion of Privacy in NSW*
- 2016 South Australian Law Reform Institute report, *A Statutory Tort for Invasion of Privacy, Final Report 4*

There is strong support amongst law reform bodies for creating a statutory cause of action to provide an adequate remedy for serious invasions of privacy.

In NSW, the most recent consideration of this issue was the March 2016 NSW Standing Committee on Law and Justice report, *Remedies for the Serious Invasion of Privacy in NSW.* Consistent with the other reports on this issue, the Committee found that available civil remedies are inaccessible, and fail to offer an appropriate remedy to people who have suffered a serious invasion of privacy. The Committee recommended that the NSW Government introduce a statutory cause of action for serious invasions of privacy based on the model proposed by the Australian Law Reform Commission report in 2014.

Existing remedies

There is currently no common law tort in Australia designed specifically to protect privacy. While the High Court of Australia has left open the possibility of the development of a common law tort[11] only a very limited number of trial courts have recognised a tort of invasion of privacy.[12] There are a number of other common law actions (trespass, nuisance and equitable action for breach of confidence) that may have application to some invasions of privacy, but these are limited in scope and remain largely untested by the courts.

In NSW, there are legislative provisions that address certain types of conduct that constitute an invasion of privacy, including the *Crimes Act 1900* (voyeurism, filming a person engaged in a private act, installing a device to facilitate observation or filming, dealing with identification information) and the *Surveillance Devices Act 2007* (unauthorised audio recording without consent). The utility of these provisions is limited to specific forms of criminal conduct.

The *Crimes Amendment (Intimate Images) Act 2017* was passed by the NSW Parliament on 21 June 2017. The Act makes amendments to the *Crimes Act 1900* in order to create a new offence for the non-consensual sharing of intimate images. Sections 91P, 91Q and 91R provide that it is an offence for a person to intentionally record or distribute, or threaten to record or distribute, an intimate image of another person without that person's consent. The maximum penalty imposed is imprisonment for 3 years or 100 penalty units, or both. Section 91S enables a court that finds a person guilty of an offence against section 91P or 91Q to order the person to take reasonable action to remove, delete or destroy the intimate image concerned. The NSW Government implemented this legislation in response to the recommendations of NSW Parliamentary Inquiry into serious invasions of privacy.

For completeness, we note the UK government's *Online Harms White Paper* (April 2019), which examines the impacts of disinformation and looks to introduce new regulation and significant sanctions to address 'serious harms' to individuals and more broadly society. They include categories such as dissemination of terrorist propaganda, child sexual abuse, cyberbullying and the promotion of suicide.[13]

---

[11] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

[12] *Grosse v Purvis* [2003] QDC 151 and *Doe v Australian Broadcasting Corporation* [2007] VCC 281.

[13] See also the Australian Government's discussion paper on *Online Safety Legislation Reform*.

Harms arising from digital technology manifest in a range of contexts and adversely impact society. A comprehensive approach to consideration of the development of new rights that includes a statutory cause of action for serious invasions of privacy together with more effective legislative and regulatory approaches and remedies in respect of cyber fraud and cyber incidents (including use of malware and ransomware) may provide a more effective framework for assessing and ultimately responding to these existing harms as they relate to individuals, governments and the private sector.

Proposal 5: The Australian Government should introduce legislation to require that an individual is informed where AI is materially used in a decision that has a legal, or similarly significant, effect on the individual's rights.

We recognise the contribution of states and territories in supporting the objective served by this proposal to provide transparency and access to information and agree with the observation of the Commission that:

> *…AI can be more reliable at some tasks than others, this knowledge also will be useful in assessing the reliability of the decision in question.*[14]

In our view, individuals should be informed of decisions that affect them legally or otherwise and this is an important tenet of administrative law. Decisions that arise from use of AI should be transparently explained to individuals.

Within Australia, information access laws are largely directed towards government transparency and accountability. To serve this purpose their remit includes government agencies broadly categorised as:

- Government Departments
- Local Councils
- Universities
- State owned corporations or other entities created under legislation
- Ministerial offices.

The starting point in respect of jurisdiction is therefore a defined agency that holds information. Access to that information is then secured through various provisions that operate proactively or mandate publication to information or enable access upon application. Access is provided in various ways including viewing, copying or obtaining information in written, visual or audio format. In some jurisdictions, including NSW, a new record can be created to enable access. Accordingly, the format of the information is important in facilitating or granting access.

In relation to accessing information held or applied through AI and digital technologies, broadly three important questions arise:

1. Who holds the information?
2. In what form is the information held?
3. How is information accessed?

[14] Discussion paper, 93.

The ways in which government makes decisions and delivers services is rapidly changing. Digital government; increasing partnership and outsourcing arrangements; administrative arrangements and service delivery models that transcend agencies and sectors all require the preservation of extant rights, accountability and the principles of open government.

As to transparent decision making, the NSW Ombudsman has said:

> *Members of the public are entitled to know why public officials and agencies have made decisions and taken actions. This is particularly the case where a decision or an action affects their interests. The giving of reasons is one of the basic principles of good administration and is often a requirement of procedural fairness.*[15]

The importance of informing individuals of the use of AI in decision making that impacts them (now and in the future) is to ensure they understand the sources/ bases for the decision and that it was not made arbitrarily, but made fairly. It is important to be clear what aspect of the decision was informed or developed from use of AI and the level of human intervention, ownership and authorship of an AI-driven decision. This will enable efficacy of the AI system (including any pre-programmed inputs/coding) to be questioned, challenged and modified.

Factors to be considered include the type of explanation to be provided noting that there are six main types of explanations:

- Rationale explanation
- Responsibility explanation
- Data explanation
- Fairness explanation
- Safety and performance explanation
- Impact explanation.[16]

Internationally regulators are responding to competing interests of digital innovation and rights protection through broad examination and provision of independent reports to government to provide solutions to potential conflict between these interests. That independent advice is informed by factors including:

- contextual use of technology/AI
- impact of technology/AI on individuals, government and broader society
- extant legal frameworks including rights, avenues for redress and remedies.

Information Commissioners have a legitimate and valuable contribution to make in respect to expandability and the principles that relate to explanation types.

---

[15] *Good conduct and administrative practice: Guidelines for state and local government* (March 2017).

[16] https://ico.org.uk/media/about-the-ico/consultations/2616434/explaining-ai-decisions-part-1.pdf

Following a recommendation contained in an independent review on growing the AI industry in the UK, the UK Information Commissioner has conjunction with the Alan Turing Institute issued for consultation a report entitled *Explaining decisions made with AI*.[17] Initiatives such as this recognise the value of harnessing the expertise, independence, and statutory role of Information Commissioners in information governance particularly as it applies to use of AI by government and its impact on information access rights and information governance more broadly.

As an ongoing member of Australia's Open Government Partnership Forum responsible for the delivery of information initiatives since inception, the NSW Information Commissioner has made an active contribution to information access rights in a digital context.

Within Australia a number of jurisdictions including NSW and Victoria have progressed this work to inform government deliberation regarding policy, programs and legislation. The IPC will continue to progress this work and actively contribute to further developments.

Examination of existing rights is essential in assessing new harms and the utility of legislative solutions particularly those directed to creating new rights.

The GIPA Act provides a useful model to examine the right of access in the context of outsourced service delivery. Section 121 of the GIPA Act is significant. That provision operates to require an agency outsourcing service provision to include in the contract an immediate right of access to prescribed information. In this way, the right of citizens to access information can be secured in part, when services are provided by non-government providers.

However, that provision does not operate in respect of decision making. Information access laws are directed towards promoting government integrity by enabling access to information regarding how governments provide services, apply funds and make decisions. This right should be preserved as governments increasingly use machine-enhanced technology to inform decision making either under licencing/contractual arrangements or through technology owned by government.

The operation of section 121 of the GIPA Act is detailed in response to Question C below.

Proposal 6: Where the Australian Government proposes to deploy an AI-informed decision-making system, it should: (a) undertake a cost-benefit analysis of the use of AI, with specific reference to the protection of human rights and ensuring accountability (b) engage in public consultation, focusing on those most likely to be affected (c) only proceed with deploying this system, if it is expressly provided for by law and there are adequate human rights protections in place.

[17] Ibid.

We agree that before an AI-informed decision-making system is deployed, a cost-benefit analysis is undertaken with regard to protection of human rights and ensuring accountability, as well as a risk assessment and consideration of the technology against a public interest test. This will assist in determining suitability of the system for the identified purpose and promote public trust in the government use of AI. This analysis could also take the form of a PIF or a rights impact assessment.

We also support engagement by public consultation. In June 2018, the NSW Information Commissioner released the Charter for Public Participation which provides a practical and principle-based approach for embedding public participation in agency decision-making frameworks and policy development. It brings together leading authorities and resources to build capacity and guide the NSW public sector in engaging with the community. The Commission may wish to have regard to the Charter in respect of this proposal.

Proposal 6(c) is predicated upon a review of extant legislation to uphold and promote human rights. This submission recognises the existence of a jurisdictional compendium in respect of information access rights and a unified identification of key legislative features to ensure optimal operation of information access legislation. This work was led by the NSW Information Commissioner with contributions from all Australian jurisdictions.

This proposal may also require consideration of the manner in which these systems are publicly reported. Under the GIPA Act agencies are required to include in their agency information guide (AIG) information that describes the ways in which the functions (including, in particular, the decision-making functions) of the agency affect members of the public. [18]

Other legislated reporting mechanisms include mandatory contract reporting by agencies. It is important that these accountability measures are not diminished as government deploys technology.

In respect of access to information relevant to decisions informed by AI it is important to note that the right to access information and the right to access personal information is enshrined under the GIPA Act and PPIP Act in NSW. Release rates in respect to access applications seeking personal information are detailed in the annual report on the operation of the GIPA Act produced by the NSW Information Commissioner.[19] In summary, release rates for this type of information vary between partial and full release. Release in full rates are generally less than 30% and partial release rates are generally less than 70%. There are a number of factors that influence these release rates including the aggregated manner in which information may be held which may lead to redactions.[20]

[18] GIPA Act section 20(1)(b).

[19] https://www.ipc.nsw.gov.au/information-access/gipa-compliance-reports

[20] Ibid.

Proposal 7: The Australian Government should introduce legislation regarding the explainability of AI-informed decision making. This legislation should make clear that, if an individual would have been entitled to an explanation of the decision were it not made using AI, the individual should be able to demand: (a) a non-technical explanation of the AI-informed decision, which would be comprehensible by a lay person, and (b) a technical explanation of the AI-informed decision that can be assessed and validated by a person with relevant technical expertise. In each case, the explanation should contain the reasons for the decision, such that it would enable an individual, or a person with relevant technical expertise, to understand the basis of the decision and any grounds on which it should be challenged.

We recognise the roles of states and territories in contributing to the promotion of rights including new rights. We particularly note that the proposal recognises a threshold requirement of an entitlement to an explanation of the decision were it not made using AI.

We support a 'right to an explanation'. This aligns with the right to access government information which is concerned with accountability and transparency of government.

We agree with the Commission that an individual affected by an AI-informed decision has the right to an explanation about the decision that is accurate and sufficiently detailed to enable the individual to exercise rights of review in respect of that decision. These rights should be clearly enshrined in law. However, as set out in this submission the increasing use of AI in a variety of contexts will raise different considerations that will require a principles-based approach to assessment. For example, automated discovery of patterns and correlations in data may develop using AI systems in the absence of direct programming. Accordingly, some settings will be supervised and others unsupervised.

Likewise, the application of data as a contributing factor towards decision making that has a direct and indirect impact upon individuals requires consideration, as does the overall social benefit, public value and public interest. There may be a need to consider prioritising and/or categorising explanations according to established principles.

Proposal 10: The Australian Government should introduce legislation that creates a rebuttable presumption that the legal person who deploys an AI-informed decision-making system is liable for the use of the system.

We support this proposal in-principle because it acknowledges the role of human beings in creating and implementing AI systems. Additionally, the proposals contained within this report refer to legal rights and responsibilities, avenues for redress and legal remedies. These are dependent upon accountability.

Accordingly, identification of a legal entity for the purposes of legal accountability is integral to the recommendations made within the report.

The concept of a 'legal person' with responsibility for system design, selection of data, algorithmic parameters, and maintenance/evaluation provides one mechanism to maintain accountability and preserve rights and avenues for redress. The system may be regarded as the tool to assist the human decision-maker to make a decision that affects individuals and the exercise of their rights. Accordingly, responsibility for the AI-informed decision-making system must be maintained and enshrined in law.

We agree with the Commission's preliminary view that:

> *…legal liability for any harm that may arise from reliance on an AI-informed decision should be apportioned primarily to the organisation that is responsible for the AI-informed decision. There will be situations where this is inappropriate, so this should be no more than a general rule, or rebuttable presumption, which could be displaced if there are strong legal reasons for doing so.*[21]

Proposal 12: Any standards applicable in Australia relating to AI-informed decision making should incorporate guidance on human rights compliance.

We support this proposal in-principle and suggest that human rights include privacy rights and the right to access government and personal information which are currently enshrined in state and territory laws.

As noted above, we support co-regulation and self-regulation in addition to regulation of government use of AI systems. Standards are a flexible and adaptable means for protecting rights. There may be scope for governments to partner with the private sector in developing a co-regulatory approach (noting that private companies often have expertise and ownership of technology). For example, recently the World Economic Forum (the international organisation for public-private cooperation) released the world's first government procurement guidelines for AI.[22] The guidelines were co-designed by the World Economic Forum's Artificial Intelligence and Machine Learning team and fellows embedded from the UK Government's Office of AI, Deloitte, Salesforce and Splunk. Members of government, academia, civil society and the private sector were consulted throughout a ten-month development process. The guidelines provide a set of 10 principles/guidelines to be applied by governments in their procurement process for AI solutions. Guideline 2 focuses on defining the public benefit of using AI while assessing risks. The Guidelines are currently being trialled in the United Kingdom.

We note the Commission has not reached a firm view about the potential for design, standards and certification to protect human rights in the context of AI-informed decision making. We support the Commission's proposal to undertake more work and analysis in this regard via a multi-disciplinary taskforce established to consider how human rights protection can be embedded across various regulatory measures.

[21] Discussion Paper, 98.

[22] <https://www.weforum.org/press/2019/09/uk-government-first-to-pilot-ai-procurement-guidelines-co-designed-with-world-economic-forum>

Proposal 13: The Australian Government should establish a taskforce to develop the concept of 'human rights by design' in the context of AI-informed decision making and examine how best to implement this in Australia. A voluntary, or legally enforceable, certification scheme should be considered. The taskforce should facilitate the coordination of public and private initiatives in this area and consult widely, including with those whose human rights are likely to be significantly affected by AI-informed decision making.

We support embedding in a project at the earliest stage human rights and information governance by design. We see this as an enabler of the public interest and regulatory compliance with existing rights-based laws. It is important that the design of a project includes transparency and accountability mechanisms so an individual can question and understand how the project impacts upon their rights.

Importantly, rights may intersect and the incorporation of a rights impact assessment which facilitates or mandates examination of the impact of technology upon a number of existing rights may provide a more comprehensive approach.

Privacy by Design

We note, by analogy, the importance of Privacy by Design (PbD), which is a specific approach to privacy, developed by Dr Ann Cavoukian, the former Privacy and Information Commissioner of Ontario, Canada, in the 1990s.

The PbD framework was published in 2009 and adopted by the International Assembly of Privacy Commissioners and Data Protection Authorities in 2010. The U.S. Federal Trade Commission recognised PbD in 2012 as one of its three recommended practices for protecting online privacy in its report entitled, *Protecting Consumer Privacy in an Era of Rapid Change*. More recently, PbD has been incorporated into article 25 of the *European Union General Data Protection Regulation*.

Privacy by Design is a methodology that enables privacy to be built into the design and structure of information systems, business processes and networked infrastructure. PbD aims to ensure that privacy is considered at all stages of the project life cycle from conception through to development and implementation of initiatives that involve the collection and handling of personal information. It positions privacy as an essential design feature of public sector practices and shifts the privacy focus to prevention rather than compliance.

The PbD methodology is built around seven foundational principles:

- **Proactive not reactive, preventative not remedial:** The PbD framework is characterised by the taking of proactive rather than reactive measures. It anticipates the risks and prevents privacy-invasive events before they occur.
- **Privacy as a default setting:** PbD seeks to deliver the maximum degree of privacy by ensuring that personal information is automatically protected in any given IT system or business practice, as the default.
- **Privacy embedded into design:** Privacy measures are embedded into the design and architecture of IT systems and business practices. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is thus integral to the system, without diminishing functionality.

- **Full functionality: positive-sum not zero-sum:** PbD seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, not through a zero-sum (either/or) approach, where unnecessary trade-offs are made. PbD avoids false dichotomies, such as privacy versus security, demonstrating that it is indeed possible to have both.
- **End-to-end security – full lifecycle protection:** PbD extends securely throughout the entire lifecycle of the information involved. This ensures that all information is securely collected, used, retained, and then securely destroyed at the end of the process, in a timely fashion.
- **Visibility and transparency – keep it open:** PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is operating according to the stated promises and objectives, subject to independent verification. The individual is made fully aware of the personal information being collected, and for what purposes. All the component parts and operations remain visible and transparent, to users and providers alike.
- **Respect for user privacy – keep it user centric:** PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Privacy Impact Assessment

A Privacy Impact Assessment (PIA) can often identify and mitigate the challenges that are encountered in implementing PbD.

A PIA allows an agency to identify and address privacy risks associated with their project before it is too late. A PIA is more than achieving regulatory compliance - it enhances the quality of information before decision makers and demonstrates that a project has been designed with privacy in mind.

The timing of a PIA is crucial. A PIA should be conducted early enough so that it can genuinely affect project design, yet not too early as to prevent an agency/ entity from obtaining the necessary information about the project to adequately assess any privacy risks.

There are seven key elements to achieve an effective PIA, namely:

- **Integral to an organisation's governance:** the PIA should be integrated into an organisation's governance structure and have clear guidance on who has responsibility over the PIA;

- **Fit for purpose:** the PIA should be commensurate with the potential privacy risks associated with the project;

- **Comprehensive:** the PIA should cover all privacy issues, not just information privacy. A PIA should also consider whether change is required in supporting documentation such as Privacy Management Plans, human resource policies or training material to accompany project implementation;

- **Available:** the PIA report should be publicly accessible as this demonstrates accountability. Where this is not possible, consider releasing a PIA summary report to notify and seek feedback on privacy issues;

- **Enables compliance:** the PIA must address all legal obligations, including under privacy legislation, namely, the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs) where relevant;

- **Ongoing:** the PIA should contain an ongoing review mechanism to assess privacy issues throughout the life cycle of the project; and

- **Constructive:** the PIA should support an organisation's privacy culture and reference your organisation's risk management process.

The above models for mapping and mitigating privacy impacts and risks demonstrate the means and methodology with which a human right may be built into the design of a project that uses a new technology or AI.

QUESTIONS

Question A: The Commission's proposed definition of 'AI-informed decision making' has the following two elements: there must be a decision that has a legal, or similarly significant, effect for an individual; and AI must have materially assisted in the process of making the decision. Is the Commission's definition of 'AI informed decision making' appropriate for the purposes of regulation to protect human rights and other key goals?

We support the Commission's proposed definition of 'AI-informed decision making' noting the elements of:

- a decision with legal, or similarly significant, effect for an individual; and

- AI must have materially assisted in the process of making the decision.

Embedded within this type of decision is a further definition that requires consensus, namely, what is meant by 'AI'. We note the Discussion Paper has grappled with this definition.[23] In addition, implicit in the 'decision element' of the definition is the decision-making process. We note both decision and process should be subject to review.

We note the second element of AI – 'materially assisting' – envisages automation of key elements of the decision-making process, and AI generating data which materially affects the ultimate decision.

Settling the meaning of 'AI-informed decision making' will make the process of ensuring accountability in such decision making easier.

Question B: Where a person is responsible for an AI-informed decision and the person does not provide a reasonable explanation for that decision, should Australian law impose a rebuttable presumption that the decision was not lawfully made?

We reiterate our comments in respect of proposal 10.

[23] Discussion Paper, 60.

We consider there should be accountability at law where a person is responsible for an AI-informed decision and the person does not provide a reasonable explanation for that decision. It is open for such accountability to be enlivened via existing administrative law mechanisms.

Question C: Does Australian law need to be reformed to make it easier to assess the lawfulness of an AI-informed decision-making system, by providing better access to technical information used in AI-informed decision-making systems such as algorithms?

We reiterate our comments in respect of proposals 5 and 6.

We consider there is scope to strengthen existing information access laws to better facilitate access to AI-informed decision-making, particularly where governments partner with the private sector and NGOs in using these technologies.

The application of technology to provide services, including the use of AI, is an increasingly prevalent feature of service delivery by governments. Direct and facilitative service contracts are characteristic of digital solutions in which a number of entities are involved in the provision of services to the public. There are identified barriers to access to information that derives from automation including restrictive licencing arrangements and explicability of algorithms. In these circumstances, the assertion of legal rights can be compromised. One solution to address this challenge is by providing access to information. In upholding the right to access information, individuals can understand and have confidence in how decisions are made and, importantly, assert their rights in respect of those decisions.

The object of the GIPA Act is to open government information to the public and in doing so maintain and advance a system of responsible and effective representative democratic government that is open, accountable, fair and effective. This object is to be realised by agencies authorising and encouraging proactive public release of government information (section 3(1)(a)); and by giving members of the public an enforceable right to access to government information (section 3(1)(b)).

Subsection (1)(c) under section 3 of the GIPA Act provides that access to government information is restricted only when there is an overriding public interest against disclosure.

Section 4 of the GIPA Act defines 'government information' as information contained in a record held by an agency. An agency must have an AIG which identifies the various kinds of information held by the agency (section 20(1)(d)). The guide must be made publicly available, together with an agency's policy documents (sections 6, 18(a) and 18(c)). What constitutes an agency's policy documents is set out in section 23 of the GIPA Act.

Information access laws are an important means to obtain government information, but access to technical information about AI and algorithms may be limited by the fact that the government does not hold the information or understand the information which may be enshroud in commercial sensitivity and held by non-government parties or even parties outside the relevant jurisdiction.

Section 121 of the GIPA Act contains mandatory requirements for certain government contracts to provide for immediate rights of access to information held by private sector contractors.

Where such contractual rights exist, an access application under section 9 of the GIPA Act can be made to the agency for that information, and a person has a legally enforceable right to be provided with access to the information in accordance with Part 4 of the GIPA Act, unless there is an overriding public interest against disclosure of the information.

Section 121 of the GIPA Act applies in circumstances where an agency enters into a contract with a private sector entity to provide services to the public on behalf of the agency.

Subject to certain exceptions, section 121 requires government agencies to ensure that their contracts provide them with an immediate right of access to information:

- relating directly to the performance of services by the contractor
- that is collected by the contractor from members of the public to whom it provides, or offers to provide, the services, and
- that is received by the contractor from the agency to enable the contractor to provide the services.

Section 121 mandates the inclusion of a clause to permit access to information held by the contractor. Despite the mandatory requirements of section 121, where there are no contractual arrangements in place and no immediate right of access to information, information in the possession of a contractor may not be government information held by an agency for the purposes of the GIPA Act.

We note that access to technical information may be achieved where the person requesting the information may not have sufficient technical literacy but can engage a technical specialist to interpret the technical information accessed by the person. The issue with this approach to access is that there may be lack of access to or means to engage an expert and this can have a profound affect on the accessibility of technically/AI-driven information and decisions.

In this regard, Zalnieriute et al have referred to three forms of opacity in respect of transparency and accountability applicable to AI-driven and automated decision making. These are:

- Intentional secrecy arising where technology may be a trade secret or contains data subject to privacy or data protection laws
- Technical illiteracy
- Difficulty in understanding actions of a complex learning technique working on large volumes of data because human beings reason differently to machines.[24]

[24] Monika Zalnieriute et al, 'The Rule of Law and Automation of Government Decision-Making' (2019) 82 *Modern Law Review* 425, 441 - 443.

These three elements of opacity mean:

> *…there will rarely be public transparency as to the full operation of a machine learning process, including understanding the reasons for the decision, understanding limitations in the dataset used in training (including systemic biases in the raw or 'cleaned' data), and accessing the source code of the machine learning process.*[25]

Question D: How should Australian law require or encourage the intervention by human decision makers in the process of AI informed decision making?

We consider that there should be human intervention in the process of AI-informed decision making. As we have stated already in this submission, we consider it appropriate that AI to be used as a tool to assist decision making rather than it becoming the decision-maker.

Recently in NSW, the Government introduced a camera detection system to detect illegal mobile phone use by drivers on roads. The camera detection system uses AI to analyse and identify images depicting a likely offence. Images selected by the system for adjudication are then reviewed by a human who decides if the image shows the offence. Transport for NSW gave evidence and a submission to Legislative Council Portfolio Committee No. 5 – Legal Affairs of the NSW Parliament about this AI system.[26]

There are other examples of human decision making that relies on AI/ automation:

- Robo-debt in Australia
- Data-driven risk assessment in US sentencing decisions e.g. COMPAS
- Automated student welfare in Sweden[27]
- Calculation of social housing rental subsidies in NSW.

We consider human intervention to be an essential aspect of AI-informed decision making.

Conclusion

The Information Commissioner and the Privacy Commissioner recognise that the development and implementation of new technologies and modes of service delivery have the capacity to enhance the citizen's experience of government. At the same time, these developments introduce potential new risks of harm. Maintaining the trust and confidence of citizens that their rights will be protected as these projects develop will contribute to the success of the projects.

---

[25] Ibid 443.

[26] https://roadsafety.transport.nsw.gov.au/stayingsafe/mobilephones/technology.html

[27] Zalnieriute et al, above n 5, 436 – 439.

The Commissioners emphasise the need to safeguard information access and privacy rights already enshrined in legislation. In this regard, the Commissioners recognise that the application of new and emerging technologies to government services will need to operate within existing legal frameworks as well as new ones.

The Commissioners consider there is merit in assessment by way of a 'public interest test' or rights impact assessment where governments consider the use of new technologies and AI so that they are deployed only where they promote the public good/interest and in ways that preserve human rights (including privacy and information access rights). A 'public interest test' is an enabler in the protection and management of information.

The public interest test provides a transparent and instructive framework to enable government decisions to be informed by sometimes competing interests and requirements. Decisions should demonstrate a balancing of these interests and rights in order to arrive at a defensible decision that demonstrates a comprehensive consideration of interests and rights.

Transparency in decision making, including clear legislative considerations in the decision making process contributes to open democratic government. Human rights by-design also contributes to such transparency.

As an independent regulator with expertise in information access and management, data governance and privacy, the Commissioners welcome the opportunity to make a submission to the Commission's Discussion Paper.

Yours sincerely

[redacted]

Elizabeth Tydd
Information Commissioner

[redacted]

Samantha Gavel
Privacy Commissioner