information and privacy commission new south wales

Inquiry into artificial intelligence (AI) in New South Wales

Submission by the Information and Privacy Commission NSW

20 October 2023

Elizabeth Tydd
CEO, Information and Privacy Commission NSW
Information Commissioner
NSW Open Data Advocate

Sonia Minutillo
A/Privacy Commissioner

Commissioners' signatures have not been included in this submission to facilitate public access to the submission, manage security risks and promote availability in accordance with the *Redacting signatures on public facing documents Practice Guide* published on the IPC website.

The Information and Privacy Commission NSW (IPC) welcomes the opportunity to provide a submission to the Inquiry into artificial intelligence (AI) in New South Wales.

About the IPC

The Information and Privacy Commission NSW (IPC) oversees the operation of privacy and information access laws in New South Wales.

The Privacy Commissioner has responsibility for overseeing and advising NSW public sector agencies on compliance with the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act).

The Information Commissioner has responsibility for overseeing the information access rights enshrined in the *Government Information (Public Access) Act 2009* (GIPA Act) and exercises functions under the *Government Information (Information Commissioner) Act 2009* (GIIC Act). The Information Commissioner also holds the role of NSW Open Data Advocate, in which capacity she provides advice across the NSW Government on nonpersonal data that should be released to the public.

The IPC is an integrity agency with functions that are fundamental to the preservation and advancement of representative democratic Government. Section 3 of the GIPA Act provides that the object of the legislation is to open government information to the public in order to maintain and advance a system of responsible and representative democratic Government that is open, accountable, fair and effective.

For further information about the IPC visit www.ipc.nsw.gov.au.

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

Information access rights and Artificial Intelligence in NSW

The broad Terms of Reference (ToRs) of this Inquiry reflect the pervasive influence of Artificial Intelligence (AI) on contemporary and future societies. Definitions of AI vary. For the purpose of our submission, a broad definition such as that adopted by the European Union may facilitate an inclusive exploration of these issues:

> ***'Artificial intelligence system' (AI system)*** *means a system that is designed to operate with a certain level of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of human-defined objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts.*[1]

Given these broad terms of reference, specific and general expertise will inform the Committee. In this respect I will confine my submission to matters within my jurisdictional remit and professional expertise. Accordingly, my contribution to the Inquiry will be targeted and manifest in both practical impacts examined through extant New South Wales (NSW) case law and observations of international developments in promoting and preserving information access rights in digital government.

Artificial Intelligence, in its current form, cannot exist in the absence of data. Government data is government information for the purposes of the *Government Information (Public Access) Act 2009* (GIPA) and this raw ingredient serves the function of AI. Accordingly, any examination of AI in the context of government must be informed by the fundamental right to access information under Article 19 of the Universal Declaration of Human Rights and enshrined in NSW under the GIPA Act.

Digital government has rapidly progressed in NSW, and we are a recognised leader in digital service delivery. The digital government program was stimulated by hypothecated funding. The Department of Customer Service (DCS) implemented and oversighted the governance process whilst also informing the allocations. This program, the Digital Restart Fund, also involving NSW Treasury will be examined in an Auditor General Report soon to be published.

The establishment of a finite fund of itself stimulates competition. Competition, internal and external to government has informed the NSW digital agenda. The *Digital Restart Fund Act 2020* was amended to include the taking of advice by the relevant Minister[2] to provide a measure of assurance in respect of the risk of the alienation of fundamental human rights in each separately funded project and the many projects that progressed through discrete funding stages.

The establishment of the fund and governing process has resulted in progressive technical thinking to harness the benefits of technology including AI. These arrangements have also fostered, to some degree, an alienation of the technical from the legal and governance considerations which impact the lives of the citizens served by the NSW public sector notwithstanding the requirement to seek advice from the Information Commissioner and the Privacy Commissioner. The risks presented by this fractured thinking are now well ventilated in the Australian political and administrative environment.[3]

---

[1] https://www.artificial-intelligence-act.com/#:~:text='Artificial%20intelligence%20system'%20(AI,logic%2D%20and%20knowledge%20based%20approaches%2C

[2] Digital Restart Fund Act s10

[3] Robodebt Report

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

Internationally, holistic thinking is driving digital government implementation and regulation. I identified this feature, and in particular, measures not present within NSW in advice to the former Minister for Digital and Customer Services in an AI regulatory scanning report published in October 2022.

As at the date of this submission I am unaware of the status of the options that the report presented. Accordingly, I will reference these options particularly under (k), (l) and (m) of the ToRs.

Commencing with the first relevant limb I provided commentary to address (e), (g), (l) and (k) of the ToRs.

Information Access: (e) the current and future extent, nature and impact of AI on social inclusion, equity, accessibility, cohesion and the disadvantaged and (g) the current and future extent, nature and impact of AI on human rights and democratic institutions and processes in New South Wales

The right to access information manifesting in NSW under the GIPA Act serves *inter alia* to:

- Maintain and advance a system of responsible and representative democratic Government that is open, accountable, fair and effective.[4]
- Combat corruption.
- Provide accountability in all five (5) government sectors.
- Ensure transparency of government decision-making.

Importantly the right to access information is also an enabling right. Through access to information other rights can be asserted such as contractual rights, and administrative or judicial review of government actions, decisions, practices and policies.

Governments have traditionally and are increasingly contracting with citizens. Social housing rental contracts are a mature manifestation of a government contract to provide services. Increasingly government provides direct funding: toll subsidies or rebates, disaster recovery grants, beekeeper grants are among the many examples of government payments that appear to replace re-examination and adjustment of base line costs in a dynamic market.

These grants or financial subsidies are provided to citizens and businesses alike and they may involve the calculation of an entitlement derived from a range of data including financial, industry, climatic and geographical. The data may be held by government or an external private source for example PEXA. Likewise, the calculations and predictions may be undertaken by government using government owned software or, increasingly outsourced specialist providers. In these more fragmented and complex systems of service delivery and decision-making, rights and people can be compromised. My objective is to highlight those issues through references to real people and their rights so that the Committee has visibility from the perspective of impacted citizens.

These cases exemplify a curtailing of the right to access government information in the following circumstances:

[4] GIPA Act s3

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

Social Housing Rental Subsidy Calculation

A social housing tenant sought information regarding her rental rebate calculated under an outsourced contractual arrangement. In these outsourcing arrangements the information accessible is narrowed both by contract and under the GIPA Act[5]. As a result, the information sought was not available to the social housing provider, the department, or the citizen. Accordingly, neither an explanation for the subsidy provided or a challenge to the rebate was available to the citizen.[6] This case also highlights limitations under the GIPA Act which distinguish between the provision of contractual services and those services which inform government decision-making.

Examination of the utility of strip searches in identifying and prosecuting the use of illegal substances

Redfern Legal Centre made an application to obtain information about strip searches conducted by NSW Police. The information was found not to be 'held' and therefore not provided because it was contained in different digital containers and required aggregation to be produced. The Tribunal accepted that producing this information would be a substantial and unreasonable application of the resources of NSW Police.[7] The case also highlights that contemporary record keeping practices including those that are inspired by privacy protection principles may alienate the legislated right to access information.

NSW COVID data shared with the Federal Government

The applicant sought information from a NSW government department regarding COVID data that had been shared with another Australian government department. The Tribunal applied existing authority regarding government information held in digital form in determining that digital information is not held by a government agency if it requires treatment to bring it into existence. The Tribunal also found that it is only in circumstances where access is proposed to be granted that the discretion to make a new record arises.[8] In these circumstances if information is found not to be held by an agency there is no requirement to provide access to that digital information.

Outsources software used to determine flood impacted land

A retired civil engineer with a working knowledge of how flood depths are calculated sought two "hard copy" documents relating to flood depth level reports about his property, being an engineer's plan ('item 1') and engineering calculations "of the quoted Depths 0.2 and 2.1 m" ('item 2'). The Council used an aerial software program acquired externally to calculate the flood depths rather than traditional human calculations. This information was important to the Applicant who sought to develop his property. The Tribunal was satisfied that item 1 was not held. The Tribunal order the Council to provide further reasons that might assist in understanding the 'software' decision making process.[9]

Each of these cases highlight unique adverse impacts on vulnerable communities. In part, they also demonstrate the asymmetrical availability of information favouring government.

---

[5] GIPA Act s121

[6] https://www.ipc.nsw.gov.au/case-note-obrien-v-secretary-department-communities-and-justice-2022-nswcatad-100

[7] https://www.ipc.nsw.gov.au/information-access-case-note-redfern-legal-centre-v-commissioner-police-2021-nswcatad-288

[8] *Ooi v NSW Ministry of Health [2023] NSWCATAD 107*

[9] https://www.ipc.nsw.gov.au/case-note-ireland-v-central-coast-council-2022-nswcatad-366

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

Government has harnessed technology and data to produce reports and make evaluations and predictions. However, in circumstances where this information is held in digital form, the existing line of judicial authority may preclude access to that same information by citizens.

These cases have been subject to my public, Ministerial, and parliamentary reporting.

The right to access government information and its impact upon democratic systems

The right to access information is both a fundamental human right and also a pillar of our democratic system of government. Realisation of this right and a functioning democracy is gauged by the Centre for Law and Democracy's (the Centre) Right to Information (RTI) rating system which measures both the legislative framework and safeguards but also the implementation of the legislation and outcomes of right to information decisions. This approach is necessary because "… *human rights [which] serve as the foundation for or underpin democracy, including the rights to freedom of expression, to vote and participate in governance, to access information, and to freedom of assembly and association.*[10]

A rating for the GIPA Act was undertaken by the Centre in 2023 at my request. The legislation scored 83 points from a possible total ranking of 140. Areas for improvement include the exemptions, budgetary independence, jurisdiction, and qualifications of the Information Commissioner.

Interestingly, other information access regimes specifically include private entities within the jurisdiction of the Information Commissioner. This approach arguably addresses the risks associated with the diminution of rights that occurs absent citizens' consent or knowledge as government outsources services and increasingly engages in partnerships for service delivery with external providers.

As government progressively implements digital services and machine enhanced decision-making there is an increasing need to promote the right to access information, modernise the GIPA Act and enliven the extant features of the legislation that promote access to information following a request, and also proactively in response to identified risks, for example government contracts, assets and disposals.

Importantly the GIPA Act provides that government agencies must:

- describe the ways in which the functions (including, in particular, the decision-making functions) of the agency affect members of the public.[11]

In this context, government agencies are required to proactively notify citizens when machine enhanced decision-making is applied. However, an ex-ante and ex post regulatory model is required to provide safeguards. This approach is reflected in the EU's approach to regulating algorithmic decision-making. The three fundamental requirements identified and operating to various degrees in the European Union are summarised below:

1. The right to know when automated decision-making is in use
2. The right to receive a general explanation of its application
3. The right to challenge which generally manifests as the right to receive, upon request a detailed description of how the system operates: including inputs and outputs. This right is exercised by way of request to access information.

The French Digital Republic Law provides these three safeguards (highlighted below) and a more differentiated approach calibrating risk to functions and covering both private and public sectors in respect of significant impact decisions:

[10] https://www.law-democracy.org/live/

[11] GIPA Act s20(b)

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

"The French Law regulates automated decision-making in a different manner considering three different cases: (1) automated decisions in the judicial field; (2) administrative automated and semi-automated decisions and (3) all other kinds of automated decisions with legal effects or significant effects on individuals.

For judicial decisions there is a total prohibition of semi or fully automated decision if such processing is intended to evaluate aspects of personality.

For administrative decisions there is a difference between semi-automated decisions and fully automated decisions. Fully automated decisions are prevented within the administrative appeal (Title I of Book IV of the Code of Relations between the Public and the Administration). Other kinds of administrative decisions are permitted, even if fully or partially automated, under certain conditions:

a) it does not involve sensitive data (under Article 9(1) GDPR);

b) it respects Chapter I of Title I of Book IV of the Code of Relations between the Public and the Administration, i.e. it respects administrative procedures;

c) it respects Article L. 311–3–1 of the Code of Relations between the Public and the Administration, according to which an individual decision taken on the basis of algorithmic processing shall include ***an explicit notification informing the person concerned****;*

d) the administration communicates the rules defining this data processing ***and the main characteristics of its implementation to the individual concerned upon his/her request****;*

e) the data controller ensures the control of the algorithmic processing and its developments ***in order to be able to explain, in detail and in an intelligible form, to the person concerned how the processing has been implemented in his or her individual case****.*

For ***private decisions****, no decision which has legal or significant effects on a person can be taken solely on the basis of automated processing of personal data, including profiling, with the exception of:*

1. the cases mentioned at Article 22 (2) lett. a) and c) of the GDPR, subject to the conditions mentioned at Article 22 (3);

2. and provided that the rules defining the data processing and the main features of its implementation are communicated ('les principales caractéristiques de sa mise en œuvre'), with the exception of secrets protected by law, by the data controller to the person concerned, upon his or her request"[12]*.*

Information access rights as they manifest in digital government are also under consideration within Australia and vigilance is required to assess the impact of this approach under our federated model of government. One of the recommendations contained in the Review of the Commonwealth Privacy Act 1988 (the Review) (19.1) recommends that the notice of use of automated decision-making is incorporated within privacy law. My response to the Review as relevant to the right to be notified of the use of automated decision-making is set out below:

> Proposal 19.1 - Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights

[12] https://www.sciencedirect.com/science/article/pii/S0267364918303753#sec0032

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

As a second tranche right to information statute, the GIPA Act reflects the indicators prescribed in the UNESCO Right to Information Rating Index and provides for the proactive release of prescribed information. This statutory approach differs from the existing *Freedom of Information Act* 1982. The potency of the GIPA Act is achieved by four pathways to access information: two proactive and two reactive pathways that form a virtuous circle.

Significantly the GIPA Act provides that agencies must adopt an Agency Information Guide (AIG) and must update their AIGs at intervals of not more than 12 months and if requested consult with the NSW Information Commissioner.

Agency policies must be included in their AIGs and in particular include information that:

a) describes the structure and functions of the agency, and

b) describes the ways in which the functions (including, in particular, the decision-making functions) of the agency affect members of the public, and

c) specifies any arrangements that exist to enable members of the public to participate in the formulation of the agency's policy and the exercise of the agency's functions, and

d) identifies the various kinds of government information held by the agency, and

e) identifies the kinds of government information held by the agency that the agency makes (or will make) publicly available, and

f) specifies the manner in which the agency makes (or will make) government information publicly available, and

g) identifies the kinds of information that are (or will be) made publicly available free of charge and those kinds for which a charge is (or will be) imposed.

Within NSW these provisions are recognised by agencies and integrity entities as requiring agencies to proactively release information describing the manner in which their decisions are made within all five regulated government sectors and in circumstances of government outsourcing. The GIPA Act is technologically neutral, and according to this interpretation, machine enhanced decision-making should be captured under the GIPA Act.

These provisions operate under the permissive access regime enshrined in the GIPA Act designed with the object of opening government. Restrictive access regimes may not serve the purpose of provision of information as effectively. In this regard the Australian Human Rights Commission Report *A National Human Rights Act for Australia 2023* (Human Rights Report) recognises the benefits and principles that underpin Article 19 of the Universal Declaration of Human Rights relevant to access to government information: *Dissemination of Information, Enhancing participation and trust*. These principles squarely align with the object of the GIPA Act and other permissive regimes which operate in a cohesive way to promote access to information and curtail withholding of government information.

This alignment of Article 19 and the GIPA Act is demonstrated by the relationship between the object of the GIPA Act and the aspects of the Human Rights Report dealing with dissemination of information: Relevant information should be proactively disseminated by making it available in a manner appropriate to local conditions and taking account of the special needs of individuals and groups that are marginalized or discriminated against. This should include:

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

a) Providing information free of charge or at reasonable cost and without undue restrictions on its reproduction and use both offline and online;

b) Providing both technical information for experts and non-technical summaries for the general public;

c) Disseminating information in clear, usable, accessible, age appropriate and culturally appropriate formats, and in local languages, including indigenous and minority languages. This may entail publications in Braille, easy-to-read and plain language formats;

d) Disseminating the relevant information as widely as possible, including through the website of the relevant public authority or authorities if that method is effective. Other dissemination channels may include local print media, posters, billboards, mass media (television or radio) and other online sources; Rights holders should have access to key information to allow effective participation in monitoring and evaluating progress in the implementation of decisions.

Additionally, as recognised in the Human Rights Report and the GIPA Act monitoring, auditing, investigating and reviewing the operation of agency disclosures of information should be undertaken independently by a specialist oversight office, as provided by the GIPA Act and the *Government Information (Information Commissioner) Act 2009* (GIIC Act).

Like most information access statutes, the GIPA Act requires agencies to furnish the NSW Information Commissioner with data on an annual basis. This data is published by the Information Commissioner and informs the proactive compliance activities of the NSW Information Commissioner. In this context the specialist knowledge and skills together with the requirement to promote the object of the GIPA Act ensure that the Information Commissioner oversights compliance with the requirements of the GIPA Act in a holistic and performance informed manner.

The object of the GIPA Act clearly establishes a regime under which government information is to be provided to individuals to ensure their human rights are upheld but also to serve a collective purpose – an open, fair system of democracy. It is in this context that the right to access information held in digital form by government and for government must be upheld. Fragmentation and reorientation of this right under other statutes may serve additional purposes but complementarity of regimes that recognise the pre-eminence of access rights under the GIPA Act[13] have provided the foundation from which an open and accountable democratic government can be fostered and that approach should continue.

Additionally fracturing the right to access personal and other government information does not recognise the contemporary government environment in which personal and 'other' information is stored collectively by agencies.

Similarly, government decision making will not, in most cases focus on inputs relevant to one individual. Accordingly, enshrining protections in privacy statutes will not provide transparency in relation to government decision making that is informed by AI.

[13] PPIP Act s5 s20(5)

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

Information Access: (l) whether current laws regarding AI in New South Wales that regulate privacy, data security, surveillance, anti-discrimination, consumer, intellectual property and workplace protections, amongst others are fit for purpose and (m) recommendations to manage the risks, seize the opportunities, and guide the potential use of AI by government

The laws identified at (l) of the ToRs do not expressly identify information access laws. However, the right to information access is fundamentally impacted by the introduction of digital government broadly, and particularly, in the deployment of AI. These risks have been well identified in academic commentary and in the approaches adopted by the European Union. However, within Australia, the focus of joint regulators appears to largely omit examination of the impact on the right to access information notwithstanding the legislative regime in place to defend and promote this right. This omission is confirmed as follows:

> *The increasing adoption of AI – in particular, generative AI – could have broad-ranging benefits and risks for Australia's economy and society. As discussed below, immediate impacts of this technology include risks to consumer protection, competition, media and the information environment, privacy and online safety.*[14]

This omission is impactful and potentially harmful in the context of our democratic institutions. Critical to those institutions is the right of citizens to expect open government - transparency and accountability by those governing and the machinery of government, and the promotion of a participative democracy. AI presents a risk to government accountability that should inform any regulatory response to its application by government.

Solutions to the potential alienation of the right to access information operating internationally are identified in the AI Regulatory Scan.

The AI Regulatory Scan provides an overview of global approaches to identified risks. It then considers the regulatory environment in NSW and the treatments applied to risks arising from AI within this jurisdiction. At page 14, I identify residual risks and treatment options following the application of treatments in NSW. Further treatments are recommended in respect of the right to access information not expressly referenced in the above laws. Accordingly, I have regard to the inclusive drafting of these ToRs and consistent with my scan, I recommend evaluation of the treatment options outlined in that Scan. These options were also evaluated in terms of effectiveness.

A return on investment (ROI) approach is adopted within the scan to facilitate consideration of the regulatory burden and cost of implementation. This approach is not based upon actual costs of implementation. Ultimately treatment options are outlined against 3 categories.

1. Legislative and regulatory
2. Policy and capability
3. Governance and consensus.

In terms of current NSW laws referable to information access as they relate to AI, in summary, my recommendation under the scan are:

> *Ensure mandatory proactive disclosure of the use of AI by agencies by inclusion as open access under the GIPA Act*
>
> *Ensure that open access includes a statement of use, inputs and a description of the operation of the AI system*

[14] https://www.oaic.gov.au/engage-with-us/submissions/dp-reg-joint-submission-safe-and-responsible-ai-in-australia-discussion-paper

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

Expand information access rights under government contracted services to AI used for decision making

Include the use of AI as a factor in favour of disclosure of information under the GIPA Act to address the existing asymmetry that protects the business interests of agencies and 3rd party providers

Additional legislative recommendations are also under development and consideration as the NSW Attorney General and Minister for Customer Service and Digital have noted my submissions regarding legislative reform and approved their departments' engagement in a project to 'modernise' the GIPA Act. A number of my recommendations address the curtailment of the right to access information highlighted in the four cases studies I have included in this submission.

A number of the risks and recommendations I have identified have been confirmed.[15]

These recommendations include non-legislative recommendations particularly in the contracting of AI and supporting technologies. However, as set out in AI Regulatory Scan at page 6, the primacy of the existing legislative/regulatory context must be considered within an ecosystem that also evaluates the economic context.

Within the policy and capability category my recommendations are as follows:

Include clauses into contracts for the provision of AI to the NSW Government covering:

- *government/purchaser right to audit/audit logs;*
- *notification requirements in circumstances of adverse impacts including complaints or legal action;*
- *access to user manuals;*
- *training data;*
- *retain government data inputs;*
- *address intellectual property rights;*
- *require monitoring to ensure currency of explainability and transparency in AI functioning.*

Accelerate AI capability development (incl. a human in the loop approach) within the NSW public sector through enhanced relationships with industry and academic experts.

Establish a live repository of AI, use, purpose, outcomes, and host agency to facilitate real time monitoring.

There are two elements of these recommendations that require further explanation because of the capacity they offer in managing identified and latent risks associated with the use of AI by government.

1. Contracts

   Under the GIPA Act outsourcing of government functions gives rise to an immediate curtailment of citizens' right to access information. The GIPA Act prescribes a limited amount of information that service providers must provide to the agency for the agency's consideration in response to a related public access application.

[15] Government Automation, Transparency and Trade Secrets; Rita Matulionye.

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

Additionally, the relevant provisions of the GIPA Act also provide the external service provider with the basis for a claim of financial and commercial interests.[16] Such claims under the GIPA Act, as observed in academic commentary, operate more broadly than analogous trade secret laws. Accordingly, agency decision makers will apply a lower threshold to withholding information that is subject to such a claim under the GIPA Act.

Increasingly traditional government services are outsourced to private providers. This practice introduces new risks including the curtailment of the right to access information. More broadly, it also impairs the compact between government and the citizens it serves when exercised absent public debate; thereby undermining trust and ultimately democracy.

The outsourcing of government services may occur in the context of public and political debate. In these cases, our system of participative democracy is preserved. However, advances in technology that inform government decision-making and service delivery are ubiquitous. In many cases technology can be so efficient and effective that governments are compelled to engage technology through outsourcing arrangements which may through opacity and accretion significantly impact citizens' rights and undermine democracy.

There is another dimension of the intersect between the GIPA Act and technology that also requires close examination. Under the GIPA Act a distinction is drawn between the function served by outsourcing arrangements.

That distinction is at the very heart of governments' use of technology either for service delivery or to enhance decision-making.[17] The relevant provision of the GIPA Act dealing with outsourcing requirements confines itself to services and it has been argued that any decision-making function that is undertaken through outsourcing arrangements will not attract the preservation of the right to access information under the GIPA Act.[18] This narrow construction is yet to be determined by NCAT. Should this interpretation prevail the GIPA Act may be regarded as outdated. The provision of government services and inputs to government decision-making have evolved radically since 2009. I have brought this potential deficit to the attention of the Ministers responsible for the GIPA Act.

Accordingly, contracts involving the use of AI, the majority of which involve machine enhanced decision-making, require a holistic review to preserve the rights of citizens. Similarly, the GIPA Act should be examined against the prevalence of contractual arrangements in NSW to identify the magnitude of the adverse impact of these arrangements on citizens' rights. From this vantage point, amendments to the GIPA Act and in particular section 121, may resolve this alienation of statutory rights.

2. <u>A repository to facilitate overarching visibility and importantly real time monitoring</u>

A significant recommendation contained in my scan of the global regulation of AI is the implementation of mechanisms to ensure visibility over agencies' use of AI. Currently as identified by the NSW Ombudsman, little is known about the uptake of machine enhanced decision-making in NSW. Applications vary from intuitive online forms to generative AI systems yet there is limited information about the types or application of these technologies both inside a portfolio and from an overarching sector wide regulatory perspective.

[16] GIPA Act s121
[17] GIPA Act s121(1)
[18] O'Brian

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

Digital regulators recognise that a comprehensive approach to regulating AI is at the core of ensuring these tools operate safely and responsibly.[19]

Lack of, or limited visibility of these technologies present significant risks to government including:

- entering into contracts absent consideration of whole of government direction, prioritisation, responsibilities and requirements
- lack of consistent specifications to meet fundamental government requirements
- asymmetrical bargaining powers favouring vendors
- failure or delays in adverse event notification by vendors to government purchasers
- unmitigated systemic harms
- an escalation in unintended harm
- accountability failures
- unnecessary complexities and barriers for regulators and importantly investigators
- remediation delays
- absence of audit trails
- absence of or limited real time monitoring of inputs and outcomes
- risks to operational integrity
- cybersecurity failings.

There are mandated open access requirements under the GIPA Act that are relevant to transparency and accountability in the context of AI. In summary, agencies are required to:

- Publicly describe the ways in which functions, in particular decision-making functions affect members of the public[20]
- Maintain a register of contracts and make contracts publicly available[21]
- Publicly describe the various kinds of government held by the agency[22]
- Publicly report on major assets (other than land holdings), appropriately classified and highlighting major acquisitions during the previous financial year.[23]

Collectively these mandatory open access requirements provide visibility over expenditure, contractual arrangements, major asset holdings and disposals. Technology can be applied to efficiently monitor mandated, open access because it must be available on a government website. This legislative feature can be harnessed to facilitate timely and effective monitoring by regulators and integrity agencies.

[19] https://www.oaic.gov.au/engage-with-us/submissions/dp-reg-joint-submission-safe-and-responsible-ai-in-australia-discussion-paper
[20] GIPA Act s. 20(1)(b)
[21] GIPA Act Part 3, Div. 5
[22] GIPA Act s.20(1)(d)
[23] GIPA Reg cl 6(2)(a)

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

Regulation of AI and its adverse impacts can only be achieved by effective oversight. Under the GIIC Act the Information Commissioner must report annually on the operation of the GIPA Act across all sectors.[24] Reporting by the Information Commissioner is made possible by the reporting regime set out in the *Government Information (Public Access) Regulation 2018* (the Regulation). Such reporting is a feature of information access statutes globally to measure the levels and types of information access provided by governments to the citizens they serve.

The Information Commissioner's annual report on the operation of the GIPA Act is now a well-established regulatory tool that:

- facilitates identification of trends, risks and actual harms
- is used to benchmark throughout Australia under the nation metrics I initiated with my fellow Commissioners/Ombudsmen, and
- informs operational, policy and legislative amendments.

An annual reporting approach such as that established under a mandatory reporting regime would serve government and citizens alike in facilitating transparency, accountability, and effectively regulating government's use of AI.

Two options exist in respect of this approach to reporting. Firstly, the information could be generated by each agency and reported centrally by an independent oversight body (or coalition of regulators). Alternatively, it could be collected from a central repository and reported upon by the oversight body. In practice reporting to inform the annual GIPA report is modelled along the lines of the first approach, with data being provided by the Information Commissioner to the public and agencies alike via the GIPA Dashboard. In this way oversight is transparent, real-time, and purposeful.

These provisions and the capacity of the GIPA Regulation to responsively prescribe open access information reflect the intention to mandate the release of government information. It is this proactive and permissive regime that provides the vehicle for accountability and transparency. Access to information regarding government's application of AI is best served by the objects and principles of the GIPA Act and more prescriptive provisions would curtail ambiguity and put vital information in the hands of citizens. This approach has at its heart, democratic values. Accordingly, the risks of misinformation can be debilitated through access to sources of truth.

Information Access: (k) the measures other jurisdictions, both international and domestic, are adopting in regard to the adaption to and regulation of AI (l) the successes and positive precedents experienced by other jurisdictions, both international and domestic, to better understand best practice

Under the category Governance and Consensus contained in the Scan at page eighteen (18) I have identified three recommended treatment options:

1. *Ensure GIPA Act annual reporting on open access requirements includes a statement of AI application and operation general description of its use by agencies to allow oversight and compliance monitoring by the Information Commission and others.*
2. *Facilitate a whole of government approach to ongoing monitoring of the application, operation and output of AI systems deployed by NSW agencies.*
3. *Engage at a national and international level to: promote consistency of regulation, governance, influence market place behaviours and advance the consideration of harmful and potentially prohibited use of AI.*

[24] GIIC Act s37

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

All of the treatment options contained in my scan of the AI regulatory environment relevant to information access are informed by global developments. The first and second recommended strategies above are detailed throughout this submission.

However, since the time of publication additional expert commentary relevant to recommendation three has been published.

> The automated decision-making recommendations arising from the Royal Commission into the Robodebt Scheme reflect the need for holistic oversight and a consistent approach to AI regulation as follows:
>
> Recommendation 17.1: Reform of legislation and implementation of regulation. The Commonwealth should consider legislative reform to introduce a consistent legal framework in which automation in government services can operate. Where automated decision-making is implemented:
>
> - there should be a clear path for those affected by decisions to seek review
> - departmental websites should contain information advising that automated decision-making is used and explaining in plain language how the process works
> - business rules and algorithms should be made available, to enable independent expert scrutiny.
>
> Recommendation 17.2: Establishment of a body to monitor and audit automated decision-making.
>
> The Commonwealth should consider establishing a body, or expanding an existing body, with the power to monitor and audit automate decision-making processes with regard to their technical aspects and their impact in respect of fairness, the avoiding of bias, and client usability[25]

Within our federated model of government, consistency is ensured through a harmonious approach. The development of the Australian Consumer Law reflects that approach. Building upon existing structures and statutes will also enable Australia to move more rapidly to address the impending harms of AI whilst also harnessing technology to serve a greater good. This public purpose approach is reflected in the existence of information access statutes throughout Australia and the extant oversight mechanisms including the role and advocacy of the Association of Information Access Commissioners.

These existing mechanisms offer ready solutions to some of the risks associated with the deployment of AI by government and should be engaged to inject oversight and build confidence and trust in government decision-making and service delivery.

[25] https://robodebt.royalcommission.gov.au/system/files/2023-07/report_of-the-royal-commission-into-the-robodebt-scheme.pdf

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

Privacy rights and Artificial Intelligence in NSW

Privacy: e) the current and future extent, nature and impact of AI on social inclusion, equity, accessibility, cohesion and the disadvantaged and (g) the current and future extent, nature and impact of AI on human rights and democratic institutions and processes in New South Wales

New and emerging technologies, many driven by AI, have changed the way citizens interact and transact with both the private and government sectors. AI systems have the potential to radically shift the way governments undertake their traditional functions. AI can, and in many cases has, enabled the public sector to improve the way it operates; enabling improved data analysis and insights, targeted delivery of essential programs and efficient and effective services that centre the customer experience. AI technologies and AI driven government decision-making systems present governments with a range of opportunities for enhanced service delivery, as evidenced by the proliferation of new machine enhanced NSW Government projects which have come to the IPC through the Digital Restart Fund (see p. 17, for recent projects under the Digital Restart Fund).

However, AI technologies also have the potential for privacy risks in which a lack of human oversight and poor system design and governance, which if left unmitigated, has the potential to lead to a range of adverse outcomes for human rights and democratic processes. These risks include:

- the incidental collection of personal information
- unauthorised use of personal information for purposes not for which it was collected
- the risk of unauthorised access to personal information
- potential for increased risk of data breaches (and harms), as large volumes of data and insights are collected and retained
- inability to properly understand how personal information is being handled as a result of the complex nature of the technology systems deployed
- inaccurate or inappropriate decision-making.

Fortunately, just as the GIPA Act provides agencies with a framework for mitigating risks to citizens' information access rights, the *Privacy and Personal Information Protection Act 1998* (PPIP Act) provides protections for citizens' privacy rights.

Under the PPIP Act, NSW public sector agencies, statutory bodies, universities, and local councils must comply with the 12 Information Protection Principles[26] when they collect, store, use or disclose personal information. When providing advice to agencies developing AI projects that use personal information, in accordance with these principles, the IPC encourages agencies to undertake a range of mitigation strategies which include the following:

- Undertaking a Privacy Impact Assessment (PIA) to map information flows, assess the project against NSW privacy laws and help to identify and mitigate privacy risks before a project proceeds. PIAs should consider the potential harms and impacts to an individual/s and identify protections that can be built into the project adopting a privacy by design approach.

[26] Information Protection Principles (IPPs) for agencies (nsw.gov.au)

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

- Developing appropriate policies and procedures, which include requirements for privacy compliance, to govern the use of any new technology in their operations, including consideration of the NSW AI Strategy, the NSW IoT Policy, NSW Cloud Policy and the Smart Places Strategy.
- Implementing access controls to limit the number of staff who have access to any personal information that is collected, with access audit logs also maintained to ensure accountability and transparency.
- Ensuring that a data breach policy is in place, with clearly articulated responsibilities, including training on privacy and data security for all staff handling personal information.
- Agencies must take steps to ensure adequate consultation with relevant Cyber Security stakeholders, including alignment with the NSW Cyber Security Strategy and the undertaking of cyber security risk assessments. Procurement contracts should also include appropriate clauses to meet Cyber Security requirements, while contracts with third party vendors should include provisions requiring compliance with privacy laws.

Additionally, in any circumstances where personal information is used that are likely to have a non-trivial impact on the citizen, ensuring that the principles of human centred design are upheld and humans are kept within the decision-making process are likely to mitigate any personal information risks perpetuated by AI systems.

Privacy: (I) whether current laws regarding AI in New South Wales that regulate privacy, data security, surveillance, anti-discrimination, consumer, intellectual property and workplace protections, amongst others are fit for purpose

In NSW, both the PPIP Act and the *Health Records and Information Privacy Act 2002* (HRIP Act) provide the framework and responsibilities for NSW Government agencies and the rights of individuals. Central to the framework are the Information Protection Principles (IPPs) and the Health Privacy Principles (HPPs) which follow an 'information life cycle' as agencies collect personal and health information, process, store and share or dispose of it. The IPPs and HPPs are complemented by other mechanisms including codes of practice (where applicable), privacy management plans and complaints management mechanisms. See both the Information Protection Principles (IPPs)[27] and Health Privacy Principles (HPPs)[28] for more information.

Together, these Acts provide a foundation for governing and upholding citizens' personal and health information privacy rights and are central to governing any government AI systems within NSW that handle citizens personal and health information. Under the PPIP Act, personal information is defined as:

> *"Information or an opinion (including information or an opinion forming part of a database and whether or not in a recorded form) about an individual whose identity is apparent or can be reasonably be ascertained from the information or opinion".*

Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics (section 4(2)).

Personal information could include:

- a record which may include an individual name, address and other details about you
- photographs, images, video or audio footage of an individual and

[27] Information Protection Principles (IPPs) for agencies (nsw.gov.au)
[28] Health Privacy Principles (HPPs) explained for members of the public (nsw.gov.au)

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

- biometrics information, fingerprints, blood or DNA samples.

Health information[29] is defined as:

(a) personal information that is information or an opinion about—

  (i) the physical or mental health or a disability (at any time) of an individual, or

  (ii) an individual's express wishes about the future provision of health services to him or her, or

  (iii) a health service provided, or to be provided, to an individual, or

(b) other personal information collected to provide, or in providing, a health service, or

(c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or

(d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or

(e) healthcare identifiers

Under the existing definitions, the legislation makes it very clear that any inputs into an AI system which involve the collection, storage, use or disclosure of the above personal or health information are bound by these Acts, and subject to the IPPs and HPPs. In this regard privacy laws already provide a regulatory framework for AI. However, the breadth of, and continuous evolution of the technology, necessitates that any approach is responsive to the pace of an ever-evolving technological landscape that is not restricted to a point in time. As a result, privacy laws in NSW should strive to remain technology neutral.

The existing regulatory framework in NSW provides a robust system for privacy and personal information governance in the age of AI, with a range of policy frameworks also underpinning the above legislative frameworks. These policy frameworks do provide the basis for a more flexible and proactive response to the regulation of AI through the promotion of rights-based principles and risk mitigation strategies to reduce any privacy risks associated with AI. In this approach, agencies are strongly advised to adopt a precautionary and risk weighted approach to the development of an AI system, with a focus on maintaining robust internal governance and accountability processes. These policy frameworks include the following:

The NSW AI Strategy: The NSW Government AI Strategy is focused on harnessing the benefits of AI to improve service delivery and government decision-making. Under the strategy, AI will not be used to make unilateral decisions that impact NSW citizens or their human rights, and the NSW Government must carefully monitor the consequences of decisions that AI might inform. The NSW AI strategy is underpinned by a suite of measures which include the NSW Artificial Intelligence Assurance Framework, the NSW Artificial Intelligence Ethics Policy, the NSW Cyber Security Policy, and the NSW Government Data Strategy.

[29] Section 6, HRIP Act

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

The NSW Artificial Intelligence Assurance Framework: The IPC was consulted on the AI Assurance Framework and provided input into its design, considering a number of the aforementioned information access and privacy issues arising within the AI landscape. The Framework provides a mandatory process for agencies to self-assess their AI projects against, to ensure that they are designed with and monitored against explicit standards for performance, reliability, robustness and auditability, and that they align with the NSW Government's Ethical AI Principles. The Framework assists project teams using AI to comprehensively analyse and document their projects' AI specific risks. It also assists teams to implement risk mitigation strategies and establish clear governance and accountability measures.

The NSW Artificial Intelligence Ethics Policy: The Policy sets out five overarching principles that are designed to ensure best practice use of AI, focusing on trust, transparency, customer benefit, fairness, privacy, and accountability. The Policy provides that AI must be the most appropriate solution for a service delivery or policy problem, and used in such a way as to mitigate as much potential bias as possible, as safely as possible, and in line with existing privacy and information access requirements (i.e. compliance with the GIPA Act, PPIP Act, and HRIP Act).

Under this policy, AI will not be used where there is not a clear use case for doing so, or where its use might pose risks in relation to data, privacy, or assurance. This approach is informed by the extensive work on AI in other jurisdictions within Australia and internationally such as the European Union, UK, and OECD. It has also been informed by detailed consultation with the community, non-government organisations, government agencies, academia and with industry.

Principles within the policy include:

- **Community benefit:** AI should deliver the best outcome for the citizen, and key insights into decision-making
- **Fairness:** Use of AI will include safeguards to manage data bias or data quality risks
- **Privacy and security:** AI will include the highest levels of assurance
- **Transparency:** Review mechanisms will ensure citizens can question and challenge AI-based outcomes
- **Accountability:** Decision-making remains the responsibility of organisations and individuals

The best use of AI will depend on data quality and relevant data. It will also rely on careful data management to ensure potential data biases are identified and appropriately managed.

AI solutions that rely on sub-optimal quality data may result in sub-optimal project outcomes and recommendations and potential harms. Algorithms that contain systemic and repeatable errors may also lead to prejudiced decisions or outcomes. Projects should clearly demonstrate a data model that is designed with a focus on diversity and inclusion, use of a dataset that is representative for the problem to be solved, and regular monitoring of data models and outputs.

The Ethics policy also places privacy and security front and centre as principles to ensure that AI will include the highest levels of assurance to ensure that data used for AI projects is used safely and securely, and in a way that is consistent with privacy, data sharing and information access requirements. Any project outcome will be undermined by lack of public trust if there is any risk of a data breach or that personal data could be compromised.

Projects must also clearly demonstrate incorporation of privacy by design principles, explaining how information privacy (including the risk of reidentification) and cyber security risks have been addressed. They must also achieve agreement on the consent for data use, with sufficient information provided on how the data will be used to ensure informed consent is realised.

The OAIC Community Attitudes Survey found that Australians are cautious about the use of AI to make decisions that might affect them, with 96% saying there should be some conditions in place before AI is used in this manner, such as the right to have humans review the decisions being made, and the requirement of a right to request information about how AI decisions are made [30].

Given the rapidly evolving and dynamic nature of technological development, policy frameworks should not seek to regulate AI projects through limitations or requirements on the specific types of technology being used and being deployed. Rather, policy approaches should seek to regulate the implementation and development of processes involved in bringing a product or system into use.

A regulatory approach in which principles underpin processes through which AI systems are brought to market would help to ensure that the conditions on the use of AI are met. This would include the right to information access, human review, and a strict adherence to privacy laws, as well as the assurance that all necessary security protocols and due diligence is being undertaken. As an example, the EU's Artificial Intelligence Act proposes to establish a technology-neutral definition of AI systems in EU law and to lay down a classification for AI systems with different requirements and obligations tailored on a 'risk-based approach'. Under this definition, some AI systems presenting 'unacceptable' risks are prohibited, while a wide range of 'high-risk' AI systems may be authorised, but subject to a set of requirements and obligations to gain access to the EU market.

Currently, the IPC adopts several risk-based principles in our approach to regulating AI projects, recommending that prior to implementing digital projects which use and handle citizen's personal information, that NSW agencies should undertake a Privacy Impact Assessment (PIA). There is scope in NSW to consider the mandatory use of PIAs for certain high-risk projects as is the case under the European Union's (EU) General Data Protection Regulation (GDPR), which is discussed in further detail below under section (m).

ID Support NSW: In October 2021, the NSW Government established ID Support, an Australian first identity support and remediation service. ID Support assists government, industry and customers of NSW, if they've experienced a data breach, if their personal information or government issued identity credentials are compromised. ID Support undertakes a range of proactive activities such as providing strategic advice and guidance on data, privacy, and cyber education, free community learning modules and education sessions, as well as free and on demand support for citizens whose proof of identity credentials are stolen or fraudulently used. ID Support is an example of a key service arising out of a need to mitigate the harms of cyber and data breaches.

NSW Cyber Security Policy: The NSW Cyber Security Policy outlines the mandatory requirements to which all NSW Government departments and Public Service agencies must adhere, to ensure cyber security risks to their information and systems are appropriately managed. This Policy applies to; information, data and digital assets created and managed by the NSW public sector, including outsourced information, data and digital assets; information and communications technology (ICT) systems managed, owned or shared by the NSW public sector; and, Operational Technology (OT) and Internet of Things (IoT) devices that handle government data, government held citizen data or provide government services.

[30] Australian Community Attitudes to Privacy Survey 2023 | OAIC

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

With government held information, data, and digital assets being integral to an AI based technology, the NSW Cyber Security Policy will also by definition apply to any AI based system. This policy is not mandatory for state owned corporations, local councils, and universities; however, it is recommended for adoption by these organisations as a foundation of strong cyber security practice.

Under the policy, agencies must manage their risk by ensuring cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle (SDLC). Any upgrades to existing systems must comply with agency's cyber risk tolerance. Audit trail and activity logging records are determined, documented, implemented, and reviewed for new ICT systems and enhancements, and ICT systems and assets are monitored under this policy to identify cyber security events and verify the effectiveness of protective measures.

NSW Government Data Strategy: The NSW data strategy ensures that the NSW government is well placed to understand the value of government held data, influencing how it is managed and protected, and that investment in data across the sector is strategic and coordinated. The strategy achieves this by recognising data as a significant state asset in its own right; aligning on standards and practices to promote consistency and increase the visibility, usability and value of data. The strategy ensures the NSW government achieves better use of data by developing deidentified enduring data assets that bring together data from across government to enable collective problem-solving, while also developing a spend category for government procurement of data and data services to ensure expenditure on data is transparent.

The Policy also strives to strengthen transparency and trust in the way that governments collect, manage, use and share data in accordance with the highest, privacy, security and ethical standards, to promote transparency of government and provide a platform for innovation. The policy will achieve this by protecting customer's rights, taking a 'by design' approach to data projects by assessing privacy, security, and ethical impacts, and aligning with community expectations and the individual and collective interests of citizens, including Indigenous peoples.

The strategy will consolidate whole of government data policies to accelerate safe use and sharing of data across government, including engaging with the Aboriginal Community to implement Indigenous Data Sovereignty and Indigenous Data Governance principles, consistent with the IPC's guidance to agencies, which includes the promotion of inclusive and culturally appropriate solutions when delivering digital government services.

IPC AI project advice

To date, the IPC has provided advice to NSW Government agencies on a range of digital projects bidding for funding from the NSW Government's Digital Restart Fund (DRF) which have utilised artificial intelligence technologies. Some of these projects, and the accompanying IPC advice provided to agencies, include the following:

The NSW Smart Beaches Project: The Smart Beaches project will deliver a standardised and automated reporting tool available to all lifeguard services, integrating available and emerging data sources. Cameras using image analytics will offer automated crowd counting at patrolled and unpatrolled beaches. GPS tracked rescue assets will provide automated beach status and rescue notifications; and further enhancement to the Manly Hydraulics Lab Nearshore Wave Tool will improve localised beach condition assessments. The installation of cameras on public beaches has the potential to create privacy concerns which the IPC consulted on.

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

The Sydney Olympic Park Authority (SOPA) Smart Places Sentiment Analysis: This project utilises a complex, multi-modality sentiment score regression model using the latest methods in statistical machine learning to improve decision-making around public safety intervention. The technology builds on crowd modelling systems that draw data from SOPA's existing CCTV network and aggregates this with additional data from other sources (including social media and environmental systems) to alert the SOPA team to changes in customer sentiment about places, particularly during major events and instances of 'crowded places'. Machine learning models are utilised to infer physical crowd characteristics from CCTV imagery with the goal of improving the understanding of complex human behaviour, as a spatial-temporal phenomenon.

Knowing crowd sentiment and how it varies can inform policy decisions to determine optimal investment of limited resources (lighting, cleanliness, crowd density, flow, security, signage, among others). The proposed system can estimate sentiment score in real-time from CCTV imagery, and the quantification of environment characteristics and social media streams. While the trial applies privacy-enhancing safeguards and controls to ensure that individuals are never identifiable, the system requires leveraging the latest tools in Artificial Intelligence, all of which have information access and privacy implications which were considered by the IPC.

The NSW Education Wallet Program: The Education Wallet program makes interventions across a series of points along a learner's journey through secondary school, into post-school learning and employment. The program consists of three major workstreams.

The first is the capability for all NSW secondary school students to utilise a 'Learner Passport' to aid in self-reflection and encourage better career-related conversations throughout secondary school regarding post-school pathways into employment.

The second involves the enhancement of a skills comparison tool to help learners source subsidised VET-related study that aligns with their interests and career pathways, unearthed through engaging with the Learner Passport. Finally, providing the capability for individuals to have their secondary school and Vocational Education and Training (VET) qualifications verified by the NSW Government (expected to occur via the Digital Identity & Verifiable Credentials solution) – and to curate and present these digital verifiable credentials to employers and other parties.

To mitigate the risks of privacy breaches and the misuse of personal information, the IPC provided advice to these projects which included the following recommendations:

- The recommendation to undertake a Privacy Impact Assessment to mitigate privacy risks.
- Embedding of Privacy by Design Principles into the project.
- Alignment with NSW Cyber Security Strategy.
- The expectation that employees and citizens will be notified of how their information will be used and shared.
- The request that appropriate processes should be in place for authorising access to, use, and disclosure of personal data. Access audit logs should also be maintained to ensure accountability and transparency.
- Training and guidance on privacy and security for staff accessing information.
- A data breach policy should also be in place and all staff made aware of their responsibilities to report breaches under this policy.
- Preservation of citizens' rights to know who holds information, in what format this information is held and what steps might be required to provide access to information.

- The requirement of an agency outsourcing service provision to include in the contract an immediate right of access to prescribed information and request clauses inserted into contracts to enable government agencies to:
  - Retain data rights
  - Address/limit claims of commercial in confidence by ensuring that the agency has access to the data and inputs used by the AI system
  - Audit the operation of the AI system, such as undertaking algorithmic impact assessments and revalidation
  - Facilitate access to audit logs retained by the service provider
  - Receive notice from the supplier of any adverse incident that are legal or administrative in nature, including system failures and unintended consequences
  - Waive legal rights in respect of purchaser's testing/auditing
  - Ensure the system operates within law/compliance requirements and subcontractors' compliance.

Overall, the existing NSW privacy laws, regulations and frameworks considered above have been effective to date in mitigating a range of privacy risks that arise through the proliferation of AI technologies. However, there are insights to be drawn from other jurisdictions which have identified areas for reform within their jurisdiction together with key learnings from separate jurisdictions. There are detailed in the paragraphs following below.

Privacy: (k) the measures other jurisdictions, both international and domestic, are adopting in regard to the adaption to and regulation of AI (l) the successes and positive precedents experienced by other jurisdictions, both international and domestic, to better understand best practice, and (m) recommendations to manage the risks, seize the opportunities, and guide the potential use of AI by government

As raised in the Attorney General Department's 2022 Report into the Commonwealth Privacy Act Review, notable Privacy reforms within the Automated Decision-making (ADM) space include the following:

- Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal, or similarly significant effect on an individual's rights. The obligation should extend to decisions that are substantially automated, rather than being restricted to decisions that are solely automated. Guidance should be provided to entities to clarify the meaning of 'substantially automated', which should not capture decisions where a human decision-maker has genuine oversight of a decision, reviews a decision before it is applied and has discretion to alter the decision.
- High-level indicators of the types of decisions with a legal or similarly, significant effect on an individual's rights should be included in the Act. This should be supplemented by OAIC Guidance. Information provided through privacy notices or privacy policies could include general information about the types of personal information that would be used and how the information would be weighted. Information provided to individuals on request could be more tailored to the specific individual and include an explanation of how a decision was reached. Information provided through privacy notices or privacy policies could include general information about the types of personal information that would be used and how the information would be weighted. Information provided to individuals on request could be more tailored to the specific individual and include an explanation of how a decision was reached.

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

- Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect. This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources. Providing individuals with meaningful information on automated decisions with legal or similarly significant effect would ensure individuals have sufficient understanding about the rationale for automated decisions to enable them to exercise other rights, either under privacy law, such as the right to object, or other frameworks such as administrative or discrimination law.

The European Union's (EU) General Data Protection Regulation (GDPR) is a significant data privacy and security law reform which came into effect in 2018 and imposes obligations on any organisations that target or collect data related to citizens within the EU. The key regulatory points of the GDPR include principles related to:

1. Lawfulness, fairness and transparency — Processing must be lawful, fair, and transparent to the data subject.
2. Purpose limitation — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. Data minimization — You should collect and process only as much data as absolutely necessary for the purposes specified.
4. Accuracy — You must keep personal data accurate and up to date.
5. Storage limitation — You may only store personally identifying data for as long as necessary for the specified purpose.
6. Integrity and confidentiality — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. Accountability — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

Of note, Articles 12 and 13 outline requirements for the rights of the data subject (citizens) to have access to transparent information and communication, and to have information provided to the data subject by the data controller (government or private party) where personal information has been collected and used. For example, under Article 12.1, data controllers must take appropriate measures to provide any requested information relating to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular, for any information addressed specifically to a child. The information must also be provided in writing, or by other means, including where appropriate, by electronic means. Article 13 provides that this information may include, but is not limited to, the following:

- the identity and the contact details of the controller and, where applicable, of the controller's representative
- the contact details of the data protection officer, where applicable
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- the legitimate interests pursued by the controller or by a third party
- the recipients or categories of recipients of the personal data.

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

Under the GDPR, data protection impact assessments (which share features of a PIA) are required for any new projects that are likely to involve a "high risk" to people's personal information. Data protection impact assessments are mandatory where processing involves:

- large-scale use of sensitive data
- systematic and extensive profiling
- public monitoring.

In the United Kingdom, the Information Commissioner's Office has listed other processing operations for which a data protection impact assessment is also mandatory. These include:

- innovative technology, including AI
- denial of service based on automated decision-making
- large scale profiling of individuals
- any processing of biometric data
- any processing of genetic data, other than by an individual GP or health professional for the provision of health care directly to the data subject
- "invisible processing": processing of personal data that has not been obtained directly from the data subject
- tracking of an individual's geolocation or behaviour, including but not limited to the online environment
- targeting of children or other vulnerable individuals
- risk of physical harm: where the processing is of such a nature that a personal data breach could jeopardise the health or safety of individuals.

In NSW the requirement to undertake the equivalent in the form of a Privacy Impact Assessment (PIA) is best practice but not a mandatory legislative requirement when adopting new technologies such as AI. Mandating the completion of a PIA as part of a minimum requirement in the governance framework for the introduction of any such technology is a viable responsive approach.

Further, AI projects that are likely to involve a high risk to people's personal information could be assessed against clear criteria and specified processing operation, to determine whether the projects exceed a certain threshold for risk. Overall, a harmonised approach with the Commonwealth, as well as alignment with recent developments in the EU, UK and other international jurisdictions, as well as the OECD Values Based Principles & EC Regulatory Framework Objectives, can provide the basis for continually addressing and mitigating privacy personal information risks that arise from the use of AI and automated decision-making technologies.

We hope these comments are of assistance to the inquiry. Please do not hesitate to contact us if you have any questions. Alternatively, your officers may contact Darby Judd, Senior Policy Officer by email at ipcinfo@ipc.nsw.gov.au.

Yours sincerely

Elizabeth Tydd
CEO, Information and Privacy Commission NSW
Information Commissioner
NSW Open Data Advocate

Sonia Minutillo
A/Privacy Commissioner

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au