information and privacy commission
new south wales

Enquiries: [redacted]
Telephone: [redacted]
Our reference: IPC21/A000456

17 December 2021

Australian Government Attorney-General's Department
4 National Circuit
Barton ACT 2600

By email: privacyactreview@ag.gov.au

Dear Sir/Madam

REVIEW OF THE PRIVACY ACT 1988 – DISCUSSION PAPER

I am pleased to make a submission in response to the Australian Attorney-General's Department Review of the Privacy Act 1988 Discussion Paper. This submission provides general commentary, as well as specific responses to the identified proposals and questions contained within the Discussion Paper. It follows on from my submission in November 2020 on the Issues Paper which was released for public comment at an earlier stage of the Review of the Privacy Act 1988.

As NSW Privacy Commissioner, I administer the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act) and promote awareness and understanding of privacy rights in NSW. The PPIP Act and HRIP Act establish the Information Protection Principles and Health Privacy Principles which govern the collection, security, use and disclosure of personal and health information by NSW government agencies and, in the case of the HRIP Act, private sector health providers.

I welcome the opportunity to provide further comment on the proposals in the Discussion Paper to amend the Australian Privacy Act. In the context of increased risks of privacy harm arising from more widespread use of digital technology and data by organisations, including from heightened cyber security risks, and the important role of digital technology and data in people's lives and the economy as a whole, it is important to ensure that Australia's privacy law takes account of these developments so that privacy rights are protected into the future. I look forward to the completion of the review and the Final Report.

Scope and application of the Privacy Act

The Discussion Paper recommends amending the definition of personal information in the *Privacy Act 1988* (Privacy Act) to make clear that it includes technical and inferred information:

> *information or an opinion that relates to an identified individual, or an individual who is reasonably identifiable:*
>
> *a) whether the information or opinion is true or not; and*
>
> *b) whether the information or opinion is recorded in a material form or not.*

I support this recommendation and the proposal that the amended definition incorporate a non-exhaustive list of the types of information capable of falling within the new definition. This list may include an identifier such as a name, an identification number, location data, an online identifier or one or more identifiers specific to the physical, physiological, genetic, mental, behavioural (including predictions of behaviours or preferences), economic, cultural or social identity or characteristics of the person.

Together with the further proposal of a list of factors to guide when an individual is reasonably identifiable, the proposed change to the definition of personal information will support entities to understand when the Australian Privacy Principles (APPs) in the Privacy Act will apply and assist in ensuring privacy compliance.

As I outlined in my submission to the Issues Paper, I note that the proposed changes would bring Australia in line with aspects of other jurisdictions, including the definition of personal data within the European Union's General Data Protection Regulation (GDPR). It is important to work towards harmonisation and consistency where appropriate, given the increasing cross-jurisdictional nature of information flows and the need to improve clarity for both regulated entities and citizens.

Sensitive information

I support in principle the recommendation to update the definition of sensitive information under the Privacy Act. In NSW, section 19 of the PPIP Act identifies types of personal information that in NSW are subject to special restrictions relating to the disclosure of that information.

Given the increasingly common use of certain technologies, such as facial recognition and biometric data, which can reveal personal information about an individual, it is timely that consideration is given to updating the definition of sensitive information to adapt to the challenges that new technology brings for privacy regulators. Any update to the definition of personal information, including sensitive information, should be done in a way that is as technologically neutral as possible, to ensure that there is sufficient flexibility to stay up to date with technological and other developments.

Deceased individuals

The Discussion Paper notes that if privacy protections are to be extended for deceased individuals any legislative amendments to the Privacy Act would need to be considered in light of relevant state and territory laws. I concur that any proposal to introduce privacy protections for deceased individuals should carefully consider existing legal frameworks.

In NSW, privacy laws continue to protect personal information of an individual for 30 years after the date of death. There are some limited exceptions under the HRIP Act which permit disclosure of a deceased person's health information where that disclosure is reasonably necessary. I note that other jurisdictions also have privacy protections for deceased individuals. For example, in Canada privacy protections continue to apply to the personal information of an individual up 20 years after the date of death and enable an executor or administrator of an estate of a deceased individual to access personal information if it will allow them to fulfill their legal responsibilities.

Notice and consent and additional protections

Emergency declarations

I support the proposed changes to amend the current emergency declarations powers under the Privacy Act to be more targeted by prescribing their application to entities or classes of entities, classes of personal information and acts or practices, or types of acts and practices.

I also support the amendment of the Privacy Act to permit organisations, other than Commonwealth agencies, to disclose personal information to state and territory authorities when an Emergency Declaration is in force and where appropriate safeguards for the sharing of personal information are in place.

In NSW, recent amendments to the PPIP Act and HRIP Act will provide similar exemptions for NSW agencies from the Information Protection Principles and Health Privacy Principles in emergency situations. NSW agencies are now able to collect, use or disclose personal information and/or health information if it is reasonably necessary to assist in any stage of an emergency. The new amendments in NSW have built-in safeguards, including that the personal information collected, used or disclosed can only be used for the purpose of assisting in a stage of an emergency, defined by reference to the *State Emergency and Rescue Management Act 1989* (NSW), and consent should be obtained unless it is impracticable or unreasonable to seek the consent of the individual to whom the information relates.

A further safeguard is the requirement to delete or further limit the use of personal information. Under the new provisions in the PPIP Act, NSW agencies must not hold the information for longer than 18 months unless extenuating circumstances apply or consent has been obtained. Similar safeguards also exist in NSW for the information collected by Service NSW through the COVID-19 check-in tool which require the deletion of check-in information after 28 days when it is not required for contact tracing. I am working with Resilience NSW and NSW Health to prepare guidelines to assist agencies to understand their obligations when sharing personal information in emergency situations.

Notice and consent requirements

Effective notice and consent mechanisms are fundamental aspects of privacy laws. The proposal to amend APP 5 to require notices to be clear, current and understandable brings Australia in line with other jurisdictions, notably the European Union and the United Kingdom. I also consider it appropriate that any information currently required in APP 5 notices be included in an entity's privacy policy, as a way to ensure continued transparency of how an entity handles personal information.

I also support the proposals to amend the Privacy Act to include additional requirements for notices to be clear, current and understandable in particular for any information addressed specifically to a child. I note that this proposal is consistent with proposals for the Online Privacy Bill to protect the privacy of children and vulnerable groups. As I outlined in my submission to Enhancing Online Privacy Bill Exposure Draft, children due to their age and inexperience, may lack an ability to fully understand the impacts of consenting to share their personal information or to understand complex and legalistic privacy notices.

I also support the proposal to strengthen the effectiveness of notice requirements by ensuring that an APP 5 notice is provided at or before the time of collection, or if that is not practicable as soon as possible after collection, unless the individual has already been made aware of relevant matters, or notification would be impossible or would involve disproportionate effort.

I also support the strengthening of privacy protections by amending the Privacy Act to define consent as being voluntary, informed, current, specific, and an unambiguous indication through clear action. I note that the Discussion Paper asks whether this proposal may have any implications for different sectors, such as healthcare. While I consider that consent should be obtained wherever practicable for the collection, use and disclosure of personal information, I note that there may be circumstances which make it difficult to obtain the consent of an individual, particularly in clinical settings.

This is recognised in NSW in the HRIP Act, where Health Privacy Principle 3 specifies that an organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so. Likewise, Health Privacy Principles 10 and 11 specify a limited set of circumstances when personal information can be used or disclosed for a secondary purpose, including for example, where it is impracticable or unreasonable to obtain consent, or where there is a need to use or disclose the information to lessen or prevent either a serious and imminent threat to the life, health or safety of the individual or another person, or a serious threat to public health or public safety.

Other exemptions

As I outlined in my submission to the Issues Paper, I support consideration of the proposals to remove or narrow the current exemptions under the Privacy Act for small businesses and political parties. It is important that the Privacy Act be amended to ensure that privacy protections in Australia keep in step with community expectations and other similar jurisdictions. I consider that the implications of any removal or narrowing of these exemptions should be carefully considered to ensure that the privacy risks are identified and addressed, and that small businesses and political parties are supported to encourage privacy compliance.

Right to object, including the right to erasure and/or amendment of personal information

I support in principle the introduction of appropriate mechanisms for an individual to control the use of their personal information. It is important that individuals have the opportunity to correct their personal information, and that this is appropriately balanced against other public interest considerations, particularly where there are valid reasons why personal information cannot be erased or amended. For example, this could include a legal requirement for agencies to retain certain types of information, and/or where there are competing public interest reasons such as public health and safety reasons.
In NSW, section 15 of the PPIP Act requires agencies to make appropriate amendments to personal information – whether by way of corrections, deletions, or additions – to ensure the information is accurate and, with regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading. Similar provisions exist in the HRIP Act.

Accordingly, I support careful consideration in the context of this review of grounds when an individual may object, request their personal information be deleted and/or amended, including a process for this to occur. This should be done with consideration of potential exceptions and requirement for agencies to consider a request in a timely manner and provide reasons, where appropriate, for any refusal, including outlining the complaint and review mechanisms that are available.

Automated decision-making

While not specifically raised in the Issues Paper, the Discussion Paper proposes that privacy policies include information on whether personal information will be used in automated decision-making which has a legal, or similarly significant effect on an individual's rights. I am supportive of the inclusion of information in privacy policies around the use of personal information in automated decision-making. This will promote transparency about when and how an individual's personal information will be used to influence decision-making and service provision.

I note that in NSW both the Privacy Commissioner and the Information Commissioner have legislative responsibilities under the *Digital Restart Fund Act 2020* (NSW) to assess risks to privacy and information access rights for digital government projects for which funding is being sought from the Digital Restart Fund. To assist agencies in the development of digital projects, the Information and Privacy Commission has prepared regulatory advice and guidance on the information access and privacy impacts of digital projects. Where a project utilises automated decision-making, agencies are advised to develop appropriate policy and procedures, which include requirements for privacy compliance, to govern the use of the technology in their operations. Agencies should build the project using privacy by design principles and incorporate mechanisms to preserve 'reviewability'. This may require ensuring the factors that inform an automated decision-making process are capable of being provided for review.

Regulation and Enforcement

Statutory tort for invasion of privacy

I note that a statutory tort for invasion of privacy will continue to be considered following submissions to the Discussion Paper. As I outlined in my submission to the Issues Paper, I support in principle the establishment of a statutory cause of action for invasion of privacy at the national level and note that there has been significant support for the creation a separate right of action to remedy serious invasions of privacy.

I note that the Discussion Paper outlines four potential options, including the establishment of a statutory tort of action based on the model recommended in the Australian Law Reform Commission report in 2014. Any model selected for a statutory tort for the invasion of privacy should be carefully considered to ensure that is accessible and effective in being able to remedy the harm caused as they relate to individuals, governments, and the private sector.

Notifiable Data Breach Scheme

The Discussion Paper seeks comments on the impact and effectiveness of the Commonwealth Notifiable Data Breach (NDB) scheme, including proposing an amendment to sections 26WK(3) and 26WR(4) of the Privacy Act to require an entity to set out the steps it has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates.

In NSW, a bill establishing a mandatory notification of data breach (MNDB) scheme in NSW is anticipated to be introduced into Parliament in early 2022. In designing the scheme, the working group was informed by the Commonwealth's NDB scheme. Noting that some NSW public sector agencies are currently captured by the Commonwealth scheme in part (e.g., if a breach involves tax file numbers), I have advocated for a model for the NSW MNDB scheme that is consistent with the NDB Scheme. Adopting a harmonious approach will make it easier for NSW agencies to comply with both schemes and promote streamlined processes. If passed, I note section 59N(g) of the NSW MNDB scheme will require agencies to outline what actions have been taken or are planned to ensure that personal information is secure, or to control or mitigate the harm done to the individual.

In the context of the anticipated introduction of the NSW MNDB Scheme in 2022, it is pleasing to note that submissions in response to the Review of the Privacy Act 1988 Issues Paper were largely positive about the impact of the NDB scheme in achieving its policy objective – which is to enable individuals to take action to protect themselves from harm that may result from a data breach. In addition, some submissions said the scheme had fostered transparency and accountability by incentivising entities to assess data breaches early and inform the public of their prevalence. The NSW MNDB Scheme is intended to achieve similar aims, in order to safeguard and protect the privacy of individuals in NSW.

New and Enhanced Enforcement Powers

The Discussion Paper recommends enhancing the current suite of regulatory and enforcement powers available to the Office of the Australian Information Commissioner (OAIC). The proposals include both strengthening existing provisions in the Privacy Act, such as the clarification of the operation of section 13G as it relates to 'serious and repeated breaches', and the introduction of new investigative powers, penalties and an infringement notice regime.

I support the enhancement of the OAIC's powers as the federal privacy regulator. If the OAIC is tasked with new and/or enhanced responsibilities and functions, it is essential that it is also resourced and funded appropriately so that it can make effective use of its enhanced suite of regulatory and enforcement powers.

Interaction between OAIC and state and territory privacy regulators, and establishment of Commonwealth, state and territory working group

I strongly support the proposal for continued regulatory cooperation with other states and territories across Australia in enforcing matters involving the mishandling of personal information. I note the significant cooperation amongst privacy authorities in Australia through well-established forums such as Privacy Authorities Australia, which meets to discuss significant privacy developments and trends in each jurisdiction and privacy challenges more broadly.

I note that privacy authorities in Australia also work proactively to respond to the regulatory challenges posed by COVID-19 with the establishment in early 2020 of the National COVID-19 Privacy team convened to respond to proposals impacting privacy laws with national implications. I joined with other Australian Privacy Commissioners and Ombudsmen to develop and publish the *National COVID-19 Privacy Principles.* These universal privacy principles support a nationally consistent approach to solutions and initiatives designed to address the ongoing risks related to the COVID-19 pandemic.

In this context, I also support in principle the establishment of mechanisms aimed at harmonising privacy laws across Australia where appropriate, and I would welcome the opportunity to be consulted on further developments including the establishment of a working group.

I hope these comments will be of assistance. Please do not hesitate to contact me if you have any questions. Alternatively, you may contact [redacted] or by email at [redacted].

Yours sincerely

[redacted]

Samantha Gavel
Privacy Commissioner