information and privacy commission
new south wales

Enquiries: [redacted]
Telephone: (02) [redacted]
Our reference: [redacted]

27 November 2020

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 - ISSUES PAPER

This is a submission to the Review of the Privacy Act 1988 Issues Paper prepared by the Australian Attorney General's Department. This submission provides general commentary and specific responses to identified proposals and questions contained within the Issues Paper.

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 care providers.

Nationally and internationally, privacy rights are increasingly impacted by new service delivery approaches and the use of technology. Against a backdrop of rapid social and technological change, it is timely to be considering whether existing legislation, such as the *Privacy Act 1988*, remains fit for purpose and continues to adequately protect citizens' privacy.

Definition of personal information

The issues paper notes the following recommendation from the ACCC's Digital Platforms Inquiry:

> *16 (a)The definition of personal information in the Act be updated to clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual.*

I support this recommendation in-principle, noting that the expansive definition of personal data under the European Union's General Data Protection Regulation (GDPR) provides a useful starting point for a definition that would capture a wide range of technical data.

I note the benefits of a national approach to establishing agreed definitions of key terms such as personal information, given the increasingly cross-jurisdictional nature of information flows. At present, the definitions of personal information vary between jurisdictions and between different pieces of legislation. Similarly, commonly used terms such as 'data' are often loosely and inconsistently defined and the differences between raw data and data analytics can be unclear. A national approach to definitions in the privacy space will improve clarity for both regulated entities and citizens.

Small business and other exemptions

In the context of the COVID-19 pandemic, a number of digital check-in solutions have been developed. In NSW, a check-in tool has been developed by Service NSW, which is covered by the PPIP Act and its privacy protections. However, there are a range of other check-in apps that have been created by private providers, some of which are not covered by the Privacy Act. This creates a jurisdictional gap, where consumers who provide their contact details via a check-in app may not be protected by an enforceable privacy law. This is of particular relevance in NSW, where the use of QR codes for check-in and contact tracing purposes has become mandatory in hospitality venues.

The mechanism under section 6EA of the Privacy Act which allows small businesses to voluntarily opt-in to the Act has been important in this context. I have been working closely with the Office of the Australian Information Commissioner and other state and territory privacy regulators to develop guidelines in relation to the collection of personal information for contact tracing purposes. These guidelines will encourage businesses and venues to use a check-in service provider that is covered by the Privacy Act or a state or territory privacy law. Check-in service providers that are not already covered by an Australian privacy law will also be encouraged to opt-in to coverage by the Privacy Act.

As the use of digital technology by small business expands, the risk of privacy harm to citizens, for example through data breaches, is greatly increased. In 2020, even a small business can collect, use and store significant amounts of personal information by using digital technology. The need for small businesses to collect personal information for contact tracing purposes has highlighted the privacy risks that arise from the small business exemption.

Accordingly, I support careful consideration in the context of this review of the greater privacy risks raised by the use of digital technology by small business and options for closing the regulatory gap that currently exists in relation to this.

I also note that the current exemptions that apply to small business, employee records and political acts and practices are now out of step with privacy regimes in other similar jurisdictions and I also support consideration of whether these exemptions should be removed or narrowed in scope, in order to provide greater privacy protection to citizens.

Notice of collection of personal information and consent to collection, use and disclosure of personal information

Providing notice of collection of personal information is critical to ensuring that citizens understand how their personal information will be handled and can separately give their informed consent. Even the most comprehensive of privacy notices does not replace consent, which requires that an individual's permission be sought to use or disclose their personal information in a certain way.

Digital platforms routinely collect information from individuals that is not necessary to provide the service requested. This is often done by obtaining a user's bundled consent for a large variety of data collection and use for a range of different purposes. Although the practice is increasingly common, it has the potential to undermine the voluntary and specific nature of any consent. By bundling consents in these different ways, digital platforms are not giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.

Reliance on general, blanket or bundled consent is not encouraged as best practice and may be open to challenge in courts or tribunals. An organisation should not seek a broader consent than is necessary for its specific purposes and needs, for example, consent for undefined future uses. In NSW, the Civil and Administrative Tribunal has expressed the view that a 'bundled' approach to gaining permission for the sharing of personal information, such as a patient registration form covering all circumstances for the patient's life, will not provide the specificity required for a valid consent[1].

However, I note that established notice and consent requirements may not be fit-for-purpose in the context of projects using data-informed technology, where all the ultimate uses of data may not be known. Data can be applied in an infinite number of ways to achieve an infinite number of outcomes. Some of these applications might not be within the contemplation of the individual who provides the data or the data custodian, but rather they are to be realised sometime in the future.

The issues paper raises the problem of 'information burden', highlighting the need to balance requirements around notice and consent with the risk of information overload or 'consent fatigue' for citizens. The ACCC's suggestion of layered notices or standardised icons or phrases to assist individuals to comprehend and process the data handling practices of entities may present a viable solution to this issue.

With regard to the form of consent, approaches taken in comparable jurisdictions may provide a useful model. For instance, one aspect of Canada's proposed *Digital Charter Implementation Act 2020* would see the introduction of exceptions where organisations may collect or use an individual's personal information without their knowledge or consent. This would apply in the context of business activities, where a 'reasonable person would expect such a collection or use for that activity'.

[1] *KJ v Wentworth Area Health Service* [2004] NSWADT 84 at [55], [61]; cited in *ALZ v WorkCover NSW* [2014] NSWCATAD 49

Statutory tort for invasion of privacy

I support in-principle a statutory cause of action for serious invasions of privacy at the national level, noting the cross-jurisdictional aspects of such invasions of privacy (for example online, interstate and internationally). I note the NSW Government separately expressed this view in its response to the 2016 report of the NSW Standing Committee on Law and Justice into Remedies for the Serious Invasion of Privacy in NSW.[2]

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

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

There is strong support amongst law reform bodies for creating a statutory cause of action to provide an adequate remedy for serious invasions of privacy. In NSW, the most recent consideration of this issue was in 2016 in the NSW Standing Committee on Law and Justice report (referred to above). Consistent with earlier reports on this issue, the Committee found that available civil remedies are inaccessible, and fail to offer an appropriate remedy to people who have suffered a serious invasion of privacy. The Committee recommended that the NSW Government introduce a statutory cause of action for serious invasions of privacy based on the model proposed by the Australian Law Reform Commission report in 2014.

While digital technology brings many benefits, harms arising from its implementation manifest in a range of contexts and can adversely impact individuals and society. A comprehensive approach to the development of new rights with a range of legislative and regulatory approaches and remedies, including a statutory tort for invasions of privacy, may provide a more effective framework for assessing and responding to harms as they relate to individuals, governments and the private sector.

Notifiable Data Breach Scheme

The Commonwealth Notifiable Data Breach (NDB) Scheme requires organisations covered by the Privacy Act in NSW to notify individuals likely to be at risk of serious harm due to a data breach. Although the NDB scheme is aimed primarily at federal government agencies and private sector organisations regulated by the Privacy Act, there are provisions that apply to NSW agencies. The Information and Privacy Commission has published guidance for NSW agencies to assist them in complying with their obligations to report data breaches, including under the NDB scheme.

[2] https://www.parliament.nsw.gov.au/lcdocs/inquiries/1877/160905%20Government%20response.pdf

The Information and Privacy Commission currently operates a voluntary data breach notification scheme. As a matter of best practice, NSW agencies are encouraged to voluntarily report data breaches to the Privacy Commissioner, and to affected individuals as appropriate. Building on these voluntary processes, I support the introduction of a mandatory data beach notification scheme in NSW.

A draft model for a mandatory reporting scheme in NSW has been developed by a working group of NSW agencies including the Department of Communities and Justice, the Department of Customer Service, the NSW Ministry of Health and the Information and Privacy Commission. Any mandatory data breach notification scheme introduced in NSW would be designed to complement the existing Commonwealth Notifiable Data Breach (NDB) Scheme under the Privacy Act, particularly in areas of jurisdictional overlap.

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

Yours sincerely

[redacted]

Samantha Gavel
Privacy Commissioner