information and privacy commission
new south wales

SUBMISSION TO REVIEW OF THE PRIVACY ACT 1988 – Review Report

Submission by the NSW Privacy Commissioner

31 March 2023

Samantha Gavel
Privacy Commissioner

The Commissioner's signature has 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.

I am pleased to provide a submission in response to the Australian Attorney-General's Department Review of the *Privacy Act 1988* (Cth) (Privacy Act) Review Report (Review Report).

The Review Report is the culmination of more than two years of extensive consultation and review of the Privacy Act. The review followed the Australian Competition Consumer Commission's (ACCC) 2019 Digital Platform inquiry final report which made several privacy recommendations.

The Attorney-General's Department has sought feedback on the Review Report. This submission constitutes my feedback and follows on from my previous submissions in December 2021 on the Discussion Paper and in November 2020 on the Issues Paper. Both of my previous submissions were released for public comment at earlier stages of the review of the Privacy Act.

As NSW Privacy Commissioner, I administer the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) and the *Health Records and Information Privacy Act 2002* (NSW) (HRIP) 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 respectively, 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.

Recommendations

Part 1: Scope and application of the Privacy Act

As noted in the Review Report, the Privacy Act is principles-based, and the definition of 'personal information' is a pillar of this design. The proposal for an amended definition of 'personal information' seeks to provide clarity to the definition of personal information without undermining the flexibility of the Privacy Act and the approach of incorporating principles-based and technology neutral definitions within the Act.

The Review Report calls to amend the objects of the Privacy Act to clarify that the Privacy Act is concerned with the protection of personal information[1] and that the Privacy Act recognises that there is a public interest in the protection of privacy[2].

[1] proposal 3.1
[2] proposal 3.2

The Review Report proposes to change the word 'about' in the definition of personal information to 'relates to'. This will broaden the definition of personal information but ensures that the connection needs to be a real connection. That is, it will capture information that has a relationship to an individual as opposed to information that is specifically about the individual (not any individual). It is recognised that this amendment ensures that the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote.[3] In addition, it will clarify that technical and inferred information can be personal information.

It is also envisaged that this proposal will further align Australia to the terminology used in the European Union's General Data Protection Regulation (GDPR) jurisdictions. I support the approach of the OAIC publishing guidance with respect to this provision. This proposal will increase consumer trust, reduce risk of harm in the event of a data breach, and improve interoperability with overseas privacy regimes.

I support the following further recommendations:

- as outlined in my submission to the Discussion Paper, to incorporate a non-exhaustive list of the types of information which may be personal information that will assist entities to identify information which could fall under the Privacy Act[4]. I recognise that a list of this kind will assist entities to identify whether information they hold falls within the definition of personal information. I note that the list would not be prescriptive which is consistent with the principles-based and technology neutral nature of the definition;

- to amend the definition of 'collection' under the Act to clarify that 'collection' covers inferred information and generated information, and that it is collected at the point it is inferred or generated[5];

- to amend 'reasonably identifiable' to be further defined by a non-exhaustive list of factors or circumstances to consider when determining whether an individual is reasonably identifiable.[6] I note that the range of circumstances in which entities deal with information is broad and that each entity will need to conduct the assessment in their own context and address the reasonableness of identification in that context;

- to amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, which is applied to personal information that involves treating it in such a way that no individual is identified or reasonably identifiable in the current context.[7] This will promote data minimisation as the amendment makes it clear that whether information remains de-identified can change depending on the context (e.g. identification may occur inadvertently in some cases as datasets or profiles are built up over time via linkages);

- together with the above proposal, given the risk that de-identified information could be re-identified, it should be afforded the same protections under the Act;

- extend the protections in APP 11.1, APP 8 and the proposed regulation of content targeted to individuals to require that these protections also apply to de-identified information;[8] and

- the OAIC develop guidance on obligations under APP 11 and to enhance best practice security measures in various contexts.[9]

---

[3] proposal 4.1
[4] proposal 4.2
[5] proposal 4.3
[6] proposal 4.4
[7] proposal 4.5
[8] proposal 4.6
[9] proposal 21.4

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

Overall, as outlined in my submission in respect to the Discussion and Issues Papers, the proposed changes will better align Australia's privacy laws with the GDPR and its definition of personal data. Noting the differences between the privacy laws of the Commonwealth, States, and Territories, I recognise that it is important to work towards harmonisation and consistency of laws, where appropriate, given the ever increasing cross-jurisdictional nature of information flows.

Sensitive information

The increasingly common use of certain technologies, such as facial recognition, geolocation tracking data and biometric data, can reveal personal information about an individual and should be appropriately regulated.

In relation to the following proposals concerning sensitive information, I support:

- in principle, the recommendation to update the definition of sensitive information to include 'genomic' information under the Privacy Act
- that the definition of biometric data for the purpose of the definition of sensitive information in the Act be developed in OAIC guidance and guidelines, which will enable the guidance to be updated over time to include technological advancements
- an amendment to the definition of sensitive information to replace 'about' with 'relates to' for consistency[10]. This will also demonstrate that sensitive information can be inferred from information which is not sensitive information.[11]

I support the inclusion of geolocation tracking data as a category of sensitive information and note the widespread public concern around the collection of location tracking data in Australia. The definition of 'geolocation tracking data' would include data that shows an individual's precise geolocation, which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time as personal information[12]. I support the amendment to recognise the collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent.

Deceased individuals

Since the release of the Discussion Paper, the Standing Council of Attorneys-General agreed that an access scheme for digital records after death or loss of decision-making capacity would be one of the work priorities in 2022. It is understood from the Review Report that the Standing Council of Attorneys-General will provide drafting instructions to the Parliamentary Counsel's committee for the development of uniform model legislation for a national access scheme for digital records after death or incapacity. I am actively engaged with the Commonwealth in relation to this work.

I concur with this consultative approach and consider that any proposal to introduce privacy protections for deceased individuals should carefully consider existing legal frameworks, and any reform to the Act consequent upon this work could be considered by the Intergovernmental Working Group.

[10] proposal 4.9(b)
[11] proposal 4.9(c)
[12] proposal 4.10

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

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. Recent case law in NSW has confirmed that an executor does not have the right to apply to amend or correct a deceased person's health information[13]. 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.

Emergency declarations

The proposed provisions relating to emergency declarations are intended to enhance information exchange between government agencies, private sector agencies and others in an emergency or disaster situation.

I support the following proposed amendments to the Privacy Act:

- to amend the Act to enable Emergency Declarations to be more targeted by prescribing their application to entities, classes of personal information, and types of acts and practices[14]. This will narrow the scope of information to be shared in an emergency situation and strikes a better balance between sharing personal information in response to an emergency and protecting an individual's privacy;

- to permit Emergency Declarations to be made in relation to ongoing emergencies, such as declared pandemics[15]; and

- 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 to share personal information are in place (i.e. provided that the state or territory has enacted comparable laws to the Commonwealth law to address any risks resulting from this)[16].

These provisions will further align the Commonwealth Privacy Act with NSW privacy laws after the recent amendments to the PPIP Act and HRIP Act which provide exemptions for NSW agencies from the Information Protection Principles and Health Privacy Principles in emergency situations. In NSW, public sector agencies are permitted to collect, use or disclose personal information and/or health information if it is reasonably necessary to assist in any stage of an emergency under the *State Emergency and Rescue Management Act 1989* (NSW). The recent amendments have several safeguards which extend to the protection of personal information in an emergency situation in NSW. For example, public sector agencies may not hold the information for longer than 18 months unless extenuating circumstances exist.

Proposed Exemptions

The increased use of digital technology in conducting business has also increased privacy risks posed to all businesses, of varying size. This includes businesses not engaging in complex information handling. There is an expectation in the community to protect an individual's privacy irrespective of the size of the business.

As I outlined in my submission to the Discussion Paper, I support the consideration of the proposals to remove or narrow the current exemptions under the Privacy Act for small businesses and political parties.

---

[13] *Nepean Blue Mountains Local Health District v ENY* [2022] NSWCATAP 356
[14] proposal 5.3
[15] proposal 5.4
[16] proposal 5.5

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

However, 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 managed to encourage privacy compliance.

Political parties' exemption

I note the proposal regarding the political parties' exemption to amend the definition of 'organisation' under the Act so that it includes a 'registered political party' and include registered political parties within the scope of exemptions in section 7C of the Act[17]. This would enable political parties to be required to comply with the APPs in the handling of personal information. It would also ensure that political entities act transparently about how they handle personal information by requiring them to make public a privacy policy in relation to acts or practices covered by the exemption[18].

I support the proposal that the 'fair and reasonable' test applies to political acts and practices, and the prohibition on targeting based on certain types of sensitive information and traits. This proposal would balance the need to protect personal information and the integrity of the democratic electoral process[19].

Small business exemption

In the Review Report it is noted that the small business exemption will be removed but only after an impact analysis has been undertaken. This process will properly inform what type of support small businesses would need in order to adjust their privacy practice to facilitate their compliance with the Privacy Act.

It is important that there is appropriate consultation and support mechanisms for small businesses to assist them to comply with their obligations proportionate to their risk (e.g. through a code)[20]. In particular, this consultation would assist in addressing concerns regarding the unnecessary collection of tenants' personal information by the real estate sector, and related concerns about how tenants' personal information is collected, stored, used and disclosed.

Part 2: Protections

Notice and consent requirements

Effective notice and consent mechanisms are fundamental aspects of privacy laws and play a crucial role in strengthening personal information handling practices.

I support the following proposals:

- include an express requirement in APP 5 to require collection notices to be clear, up-to-date, concise, and understandable;
- that collection notices be developed in a user-friendly way[21];
- the new definition of 'consent' in the Privacy Act to be voluntary, informed, current, specific, and an unambiguous indication through clear action[22];

[17] proposal 8.1
[18] proposal 8.2
[19] proposal 8.3
[20] proposal 6.1
[21] proposal 10.1
[22] proposal 11.1

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

- noting that the APP 5.2 list of matters should be retained[23], the OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the individual in the circumstances, need to be addressed in a notice.[24];

- the addition that standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the Australian economy[25];

- the OAIC develops guidance on how online services should design consent requests, as this guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context (and to consider further progressing consents as part of any future APP codes[26];

- to expressly recognise the ability to withdraw consent to reinforce the importance of valid consent. I note that the withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal[27];

- the online privacy settings should reflect the privacy by default framework of the Privacy Act[28]. I note the proposal includes that APP entities that provide online services should be required to ensure that any privacy settings are clear and easily accessible for users; and

- the privacy settings would be progressed as part of the Children's Online Privacy Code which would apply to online services accessed by children. I note the Children's Online Privacy Code is modelled on the UK's Age-Appropriate Design Code and introduces prescriptive standards for pro-privacy defaults in a range of settings.

Fair and reasonable personal information handling

I welcome the proposal in the Review Report for a new 'fair and reasonable' test to underpin the activities of APP entities when handling personal information[29]. This proposal is a shift from consent being the primary avenue for authorising conduct, and recognises that individuals should not have the main responsibility of ensuring that they do not experience harm as a result of an entity's information-handling practices. Instead, the onus is on the entities to ensure that personal information is handled in a fair and reasonable way and that projects are developed adopting a privacy by design approach.

I consider that the fair and reasonable test provides additional protections to reflect community expectations, increases the standard of handling of personal information, and improves consumer trust of digital services. However, I note that there may be additional complexities when applying the 'fair and reasonable' test to government agencies in the exercise of their statutory functions.

I support the proposal in principle to amend the Privacy Act to require that an entity be allowed to collect, use and disclose personal information only where it is fair and reasonable in the circumstances. The fair and reasonable test would be an objective test to be assessed from the perspective of what a reasonable person would consider appropriate in the circumstances.

[23] proposal 10.2
[24] proposal 10.2
[25] proposal 10.3
[26] proposal 11.2
[27] proposal 11.3
[28] proposal 11.4
[29] proposal 12.3

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 Impact Assessments for high-risk activities

A privacy impact assessment (PIA) is well-recognised as an important privacy by design process and a useful tool to ensure that privacy protections are built into projects from their conception through to implementation. I have published a Guide to Privacy Impact Assessments and encourage the use of PIAs by NSW public sector agencies.

The Review Report proposes that APP entities be required to conduct a PIA for activities with high privacy risks, including those involving facial recognition technology or other biometric information. This legislative requirement would be supported by OAIC guidance that articulates factors that may indicate a high privacy risk, with examples of activities that will generally require a PIA to be completed. This work would be done as part of a broader consideration by government of the regulation of biometric technologies[30].

I support this approach and recognise the need for increased regulation and continued consideration of these issues as governments and businesses are increasingly seeking to use facial recognition technology to support the delivery of services.

Research – proposal for 'broad consent'

The Review Report concludes that broad consent for research should be permitted in the Australian context to facilitate important human-based research. Adopting an approach similar to the GDPR, individuals could give broad consent for 'research areas' instead of limiting their consent to a particular project[31]. Additionally, the Review Report calls for further consultation on broadening the scope of research permitted without consent under the Privacy Act for both agencies and organisations[32] and on developing a single exception for research without consent and a single set of guidelines, including considering the most appropriate body to develop the guidelines[33]. I would welcome further consultation on these reforms given the potential overlap with NSW laws that require reporting by Human Research Ethics Committees.

Automated decision-making

The Review Report proposes that privacy policies should set out the types of personal information that will be used in automated decision-making, as this has a legal or similarly significant effect on an individual's rights[34]. It is important that an individual understand how their personal information is used to influence decision-making.

I support the following proposals:

- include high-level indicators in the Privacy Act of the types of decisions with a legal or similarly significant effect on an individual's rights. It is proposed that this statutory requirement be supplemented by OAIC Guidance[35];

- the introduction of a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made, with related information to be included in privacy policies. I note this proposal is to 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[36].

[30] proposals 13.1 and 13.2
[31] proposal 14.1
[32] proposal 14.2
[33] proposal 14.3
[34] proposal 19.1
[35] proposal 19.2
[36] proposal 19.3

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

Part 3: Regulation and Enforcement

Statutory tort for serious invasions of privacy

As I outlined in my submission in the Discussion and Issues Papers, I support in principle the establishment of a statutory cause of action for invasion of privacy at a national level and note that there has been significant support for the creation a separate right of action to remedy serious invasions of privacy, based on the model recommended in the Australian Law Reform Commission report in 2014 (ALRC Report 123). That is, that a statutory tort be enacted in a standalone Commonwealth Act rather than the Privacy Act. However, I appreciate there may be complexities that NSW public sector agencies may face regarding the implementation of a statutory tort for serious invasions of privacy, as it relates to States and Territories. I would seek to be further involved in the consultation process with the Commonwealth regarding this issue[37].

Notifiable data breaches scheme (NDB scheme)

I note the introduction of the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022*, following several high-profile data breaches, and that the legislation includes reforms to improve the utility of the NDB scheme.

In NSW, recent amendments to the PPIP Act will come into effect on 28 November 2023 and will create a mandatory notification of data breach (MNDB) scheme applicable to the NSW public sector.

The NSW MNDB scheme was designed and informed by the Commonwealth's NDB scheme. I advocated for a harmonious approach with the Commonwealth's scheme noting that NSW public sector agencies are currently captured by it in part (e.g. if a data breach leads to tax file numbers being compromised). I support the proposals to undertake further work to facilitate the reporting processes under the NDB scheme, which would assist both the OAIC and entities with multiple reporting obligations[38].

A proposed amendment to the Privacy Act would require notification to the Australian Privacy Commissioner as soon as practicable and not later than 72 hours after the entity becomes aware of an eligible data breach, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours[39]. The Review Report deems the 72 hour notification appropriate and necessary due to recent large-scale breaches and suggests that the 72 hour notification period better aligns with community expectations. This notification period also aligns with the requirements under the GDPR. While this notification period is shorter than the maximum 30 days specified for the NSW MNDB scheme, it is generally consistent with the IPC's published guidance that agencies should notify the Privacy Commissioner as expeditiously as possible.

I am pleased to note the proposals in the Review Report that will both support the NDB scheme and promote greater alignment with the NSW MNDB scheme. In particular, the proposed amendment to subsections 26WK(3) and 26WR(4) will require a statement about an eligible data breach to set out the steps the entity 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. This proposal reflects the requirements in the MNDB scheme provided for in sections 59M(2)(a) and 59O(g) of the PPIP Act. However, the proposed amendments to the NDB scheme would not require an entity to reveal personal information, or disclose information where the harm associated with doing so would outweigh the benefit in providing the information. The proposal for a further requirement that entities should take reasonable steps to prevent or reduce the harm that is likely to arise for individuals because of a data breach is also consistent with the MNDB Scheme, and reflects section 59F of the PPIP Act.

[37] proposal 27.1
[38] proposal 28.1
[39] proposal 28.2

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

In addition, the Review Report considers that entities should take care not to undermine the broader rationale of the NDB scheme by pursuing tailored notification at the expense of timely reporting. I note that the failure to notify individuals in a timely manner may place individuals at greater risk of serious harm. In particular, the threat of identity theft and other such crimes increases the longer that individuals are prevented from taking steps to protect themselves. I also note that the proposal requires entities to take reasonable steps to implement practices, procedures, and systems to enable it to respond to a data breach.

In addition, I note the proposal to introduce a provision in the Privacy Act to enable the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach. I note the safeguards to ensure that only limited information could be made available for a designated purpose and timeframe and to minimise the risk of harm.

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

I support the proposal for continued regulatory cooperation between the Commonwealth and States and Territories across Australia[40]. Again, I note the signification co-operation amongst privacy authorities in Australia through well-established forums such as Privacy Authorities Australia (PAA), which meets to discuss significant privacy developments and trends in each jurisdiction and privacy challenges more broadly. I also note the PAA statement in support of complaint and enforcement co-operation, which is published on the IPC's website.

I also support in principle the establishment of mechanisms aimed at harmonising privacy laws across Australia focusing on key issues[41]. I would welcome the opportunity to be consulted on further developments including the establishment of a Commonwealth, State and Territory working group.

I hope these comments will be of assistance. Please do not hesitate to contact my office if you have any questions.

Yours sincerely

Samantha Gavel
Privacy Commissioner

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

[40] proposal 29.2
[41] proposal 29.3

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