AUSCL

AUSTRALIAN SOCIETY FOR
COMPUTERS & LAW

18 June 2021

Australian Competition and Consumer Commission
By email: policy@justice.nsw.gov.au

Submission: The Privacy and Personal Information Protection Amendment Bill 2021

About us

The Australian Society for Computers and Law (**AUSCL**) is an interdisciplinary network of professionals and academics focussed on issues arising at the intersection of technology, law, and society. It is a non-profit, registered Australian charity with a charter to advance education and policy development. AUSCL was officially launched in July 2020, but its member State societies were formed as early as 1981. AUSCL provides a forum for learned discussion and debate through its Policy Lab, Working Groups and Events Program attracting support and engagement across Australia and globally.

This submission

Our submission is not intended to be a comprehensive response to all of the issues raised in the *Privacy and Personal Information Protection Amendment Bill 2021* (**PPIP Amendment Bill**), but rather focuses on specific topics on which, from our research, we can shed light.

We therefore limit our submission to the following 7 issues:

1. The scope and focus of the proposed changes
2. Definition of 'Eligible Data Breach'
3. Resourcing of the Regulator
4. Extensions to assessment periods
5. Public Notification
6. Exemption from notifications to affected individuals; and
7. Reconciliation with other data breach notification obligations.

Our submissions reflect the author's views as individuals and do not reflect the views of our employers, clients, workplace, or any other associations that we may be part of.

Scope and focus of the proposed changes

The PPIP Amendment Bill proposes to strengthen the protection of Privacy in NSW through the following reforms by doing the following:

- Creating a Mandatory Notification of Data Breach Scheme (**MNDB scheme**) to require public sector agencies bound by the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**) to notify the Privacy Commissioner and affected individuals of data breaches of personal or health information likely to result in serious harm and to satisfy other data management requirements, including to maintain an internal data breach incident register, and have a publicly accessible data breach policy.
- Applying the PPIP Act to all NSW State Owned Corporations (**SOC**s) that are not regulated by the Australian *Privacy Act 1988* (Cth) (**Privacy Act**), and
- Repealing s117C of the *Fines Act 1996* (NSW), to ensure that all NSW public sector agencies are regulated by the same mandatory notification scheme.

The MNDB scheme would apply to all 'public sector agencies' as defined by the PPIP Act. This includes all NSW agencies and departments, statutory authorities, local councils, bodies whose accounts are subject to the Auditor General and some universities. If the proposal to extend the application of the PPIP Act to SOCs is enacted, then the MNDB scheme would also apply to SOCs.

The MNDB scheme will apply to all personal information including health information within the meaning of the *Health Records and Information Privacy Act 2002* (NSW) (**HRIP Act**). Currently there is no mandatory reporting scheme for breaches involving health information under the HRIP Act and therefore we welcome the inclusion of health information as part of the MNDB scheme.

Definition of 'eligible data breach'

Inclusion of 'loss of access'

In the PPIP Amendment Bill, the definition of an eligible data breach (in s59C and throughout the Exposure Draft) has been aligned to that used in the *Privacy Act*, that is:

- unauthorised access to personal information
- unauthorised disclosure of personal information
- loss of personal information.

Noting the development of privacy law in other jurisdictions (particularly the EU), we recommend that consideration be given to including 'loss of access to personal information' to this definition (see, for example, Article 4(12) of the EU General Data Protection Regulation).

Ransomware attacks have surged globally and in Australia since 2019[1]. We also note that there has been discussion at the Federal level of requiring notification of ransomware incidents.[2]

As a State government, the NSW Government does a great deal of direct service delivery to the people of NSW and further is a leader in digital service delivery. As a result, if NSW loses access to digital service accounts (and the data in that account), this can cause harm ranging from minor inconvenience to severe harm, depending on the criticality of the service. We consider it would be prudent and future-focused to expand the definition to include loss of access to personal information, noting that there should be exclusions or exemptions for short term or planned outages, where the loss of access is expected, limited, and transitory.

[1] https://www.bitdefender.com/files/News/CaseStudies/study/395/Bitdefender-2020-Consumer-Threat-Landscape-Report.pdf
[2] https://www.innovationaus.com/labor-calls-for-mandatory-ransomware-notice-scheme/

Reasonable person

We note that an eligible data breach (in s59C and throughout the Exposure Draft) is defined to include unauthorised access or disclosure of personal information, where a *reasonable person* could conclude that the access or disclosure would be likely to result in *serious harm* to an individual to whom the information relates. However, the PPIP Amendment Bill does not provide a definition for 'reasonable person'.

The Office of the Australian Information Commissioner (OAIC) describes a 'reasonable person' as 'a person in the entity's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach'.[3] 'Reasonable person' is also discussed in general terms in Chapter B of the OAIC's APP Guidelines.

We propose that the PPIP Amendment Bill or its related Guidelines include the definition of 'reasonable person' and align this with the current definition provided by the OAIC for consistency.

'Likely' to result in 'serious harm'

The PPIP Amendment Bill does not provide a definition for 'serious harm', or when an event is considered *likely* to result in serious harm.

Serious harm is not easily defined and it needs to be assessed on a case-by-case basis.

Given the PPIP Amendment Bill will extend to include health information and government identifiers, certain types of personal information is more likely to result in serious harm than others. Previously, targeted requirements are set out by the NDB scheme under the Privacy Act to impose NDB obligations when certain types of personal information is involved (e.g. TFN data breach).

We recommend that the PPIP Amendment Bill include mandatory notification requirements if any data breaches occur involving particular types of personal information, such as Medicare number or passport details, to provide more clarity.

Mandatory notification may also be required if data breach involves a large amount of personal information (e.g. over a million records).

It will also be helpful to include accompanying commentaries or guidelines to the PPIP Amendment Bill to clarify to what extent a breach is *likely* to result in serious harm to an individual. According to the OAIC, 'likely to occur' means the risk of serious harm to an individual is more probable than not (rather than possible),[4] which essentially means when an event has a greater than 50% chance of occurring. It will be helpful to include a similar explanation in relevant commentaries to provide consistency.

We recommend that the Explanatory Memorandum of the PPIP Amendment Bill provide further details as to when it is considered to be likely to result in serious harm so that the assessor can assess the situation consistently, aligning to the Explanatory Memorandum of the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) to maintain consistency.

---

[3] Off ce of the Austra an Informat on Comm ss oner, *Data Breach Preparation and Response Guideline*, page 33.
[4] Off ce of the Austra an Informat on Comm ss oner, *Part 4: Notifiable Data Breach (NDB) Scheme*

Resourcing of the Regulator

We note that, following the introduction of a mandatory notification scheme, notifications to the NSW Privacy Commissioner are likely to increase substantially.

The experience of the OAIC with its shift from its voluntary notification scheme to the current mandatory scheme is illustrative. In the final full year of its voluntary notification scheme (FY 2016-2017), the OAIC received 114 voluntary notifications.[5] In comparison, in the first 12 months of its mandatory data breach notification scheme, the OAIC received 964 notifications.[6]

Accordingly, in order for the NSW Privacy Commissioner to be able to process the likely increase in notifications, it is critical for the NSW Privacy Commissioner's office to be resourced appropriately to not only process and log the increased number of notifications it is likely to receive, but to be able to investigate reports of particular concern to ensure that breached agencies are appropriately handling incidents to prioritise the well-being of affected individuals. In this regard, further resourcing for the purposes of training and general awareness should also be provided for.

Extensions to assessment periods

Section 59J permits the head of a breached agency to unilaterally approve the extension of the assessment period, if they are satisfied that the assessment cannot be conducted within 30 days.

In our experience, and having regard to the Federal data breach notification scheme, it is not an uncommon occurrence that data breaches are complex enough to require a period greater than 30 days to determine whether they are notifiable. As such, we support the inclusion of a mechanism to extend the assessment period.

However, we consider there is a conflict of interest in permitting a regulated entity to itself make the determination that an extension is warranted and approve the extension by its own head of the agency as set out in s 59J. In our experience, it is not uncommon for breached entities to seek to delay notification in order to limit the effect of media attention, or delay regulator action.

Accordingly, we consider that it would be preferable for extensions to be granted by the NSW Privacy Commissioner, whereby the head of the agency must seek an extension from the Commissioner, and provide reasons why the extension is required. Where the Commissioner is satisfied, they may grant the extension for an appropriate period, with monthly progress updates as envisioned by s59J(3).

Public Notification

We welcome the proposal to require that agencies establish a public notification register (in s59O of the Exposure Draft).

[5] https://www.oaic.gov.au/about-us/our-corporate-information/annual-reports/oaic-annual-reports/annual-report-2016-17/

[6] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

In the interest of transparency, we recommend that the NSW Privacy Commissioner establish its own single public register of notifications across all agencies subject to the PPIP Act, to provide the public with a single view of notifications across the NSW government.

Further, we recommend that the NSW Privacy Commissioner provide regular statistical reporting, in a similar way to the regular data breach reports provided by the OAIC.[7] These reports provide transparency and support identification of trends and formulation of appropriate responses by regulated entities and the risk and security industry.

We strongly recommend the establishment of an online notification portal (that is, a web form), that agencies can use to notify the NSW Privacy Commissioner. This should enable the standardisation of notifications, efficiency in preparation and submission of notifications and, critically, automation of data entry into the Commissioner's record management systems.

As discussed, we consider it likely that notifications under a mandatory scheme will increase substantially. Investment in appropriate digital infrastructure to minimise administrative handling will be essential, so that the Commissioner's resources may be better dedicated to supporting and (where necessary) investigating agencies experiencing data breaches.

Exemption from notifications to affected individuals

Section 59W would allow the head of an agency to exempt the agency from notifying if they reasonably believe notifications would worsen the agency's cybersecurity or lead to further data breaches.

While we agree that, in some cases, disclosing a breach may worsen a breached entity's security posture, we consider it a conflict of interest for the head of a breached agency to be in a position of granting the exemption from notification to that agency.

Accordingly, we consider that it would be preferable for any exemption from the notification requirement to be granted by the Privacy Commissioner, whereby the head of the agency must seek the exemption from the Commissioner, and provide reasons why the exemption is required. Where the Commissioner is satisfied, they may grant the exemption for an appropriate period, with monthly progress updates as envisioned by s59W(4).

Further, we consider that it would be preferable for any exemption from the requirement to be limited to the notification of affected individuals; for the purposes of accountability and statistical reporting, breached entities should still be required to notify the Commissioner. However, where the exemption is granted, the agency should not be required to list the breach on its public notification register (s59Z) unless the exemption expires.

Reconciliation with other data breach notification obligations applicable to NSW Public Sector Agencies

When creating a MNDB scheme to require public sector agencies bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of data breaches under the PPIP Amendment Bill,

[7] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/

considerations should be made regarding existing data breach notification imposed by other legislation on NSW Public Sector Agencies.

The PPIP Amendment Bill should attempt to reconcile the data breach notification obligations and minimise duplicated reporting efforts.

Data breaches involving a TFN

Any agency that collects tax file numbers (**TFNs**) has obligations under the Notifiable Data Breaches (**NDB**) scheme under the Australian Privacy Act when it experiences a data breach involving a TFN. This includes state and local government agencies and public universities in NSW that routinely collect and hold TFN information.

The notification requirements under the NDB scheme are triggered if the TFN data breach occurs where TFN information is lost, or subject to an unauthorised access or disclosure, and if the breach is 'likely to result in serious harm' to any individual. The obligations to notify are in addition to responsibilities under the PPIP Act.

Given the PPIP Amendment Bill extends the MNDB scheme to all personal information, NSW Public Sector Agencies will have to report TFN notifications to both NSW Privacy Commissioner and to the Australian Privacy Commissioner at the Office of the Australian Information Commissioner (**OAIC**). Considerations should be made to simplify the TFN notification so that only one reporting process is maintained, or to remind agencies of their obligations to report to both NSW and Australian Privacy Commissioners to maintain consistency in reporting.

Data breach notification scheme in respect of sharing of government sector data

The *Data Sharing (Government Sector) Act 2015* (NSW) (**DSGS Act**) has a data breach notification scheme in respect of sharing of government sector data under the DSGS Act with the NSW Data Analytics Centre, or between other government sector agencies.

Currently, if an agency receiving personal or health information under the DSGS Act becomes aware of any data breaches, the agency must inform the data provider and the NSW Privacy Commissioner.

Given the PPIP Amendment Bill extends the MNDB scheme to all personal information, considerations should be made to repeal the MNDB obligations imposed under the DSGS Act to keep a single source of MNDB obligations for NSW Public Sector agencies.

European Union's General Data Protection Regulation

The General Data Protection Regulation (**GDPR**) commenced on 25 May 2018 and applies to any organisation offering goods or services to, or monitoring the behaviour of, individuals living in the European Union (**EU**). This may include some NSW public sector agencies (e.g. universities offering educational packages to international students).

The PPIP Amendment Bill may consider including an additional section to stipulate that NSW Public Sector agencies should notify the NSW Privacy Commissioner within 72 hours before making any data breach notifications to the relevant EU supervisory authority under the GDPR.

Consultation

Please contact us if you would like to discuss any aspect of this submission either in person or as a round table discussion.

Yours sincerely,

[redacted]

With thanks to our authors:

[redacted]

Notice

This submission is authored by members of the AUSCL Policy Lab and Risk and Governance Workstream on behalf of AUSCL. It is intended to provide an overview of issues for consideration by the Australian Competition and Consumer Commission in relation to the proposed *Privacy and Personal Information Protection Amendment Bill 2021.* Any views expressed should not be taken to be the personal views or institutional position of the individual authors, their employers, clients, organisations, or other entities with whom they are associated.

AUSCL

REGISTERED CHARITY

IFCLA