# Providing data breach notification protections against State governments (Submission on the *Privacy and Personal Information Protection Amendment Bill 2021* (NSW))

[redacted]

2 July 2021

**Contents**



[redacted]

*Providing data breach notification protections against State governments*

The Draft Privacy and Personal Information Protection Amendment Bill 2021 (PPIP Act), is a welcome innovation of the New South Wales Government concerning the privacy of its citizens, and others with whom the NSW Government has dealings.

At present, Australian citizens living in New South Wales do not have the protections of mandatory data breach notification (MDBN) requirements in relation to data breaches by New South Wales (NSW) government agencies, or by organisations/contractors who provide services on behalf of the NSW Government, and who may not be covered by the DBN requirements of the *Privacy Act 1988* (Cth). In contrast, currently those NSW citizens whose data privacy may be breached by private sector entities or Commonwealth government agencies, have the right to be notified and to protect themselves against the consequences of such breaches. Noting that the vast majority of Australian (83%) want more governmental action to protect the privacy of their data[1], this submission supports NSW citizens being given such rights, and in a form which gives stronger protection than the current draft Bill.

We focus in this submission upon those areas of the Bill requiring amendment to provide NSW citizens the protections they deserve and which will help to restore and enhance the reputation of NSW for privacy respectful governance and regulation. Each issue we identify commences with a brief rationale with supporting evidence, followed by our recommendations.

We find that the draft Bill, while in theory an important advance for citizens of NSW, delivers a far more limited and defective set of reforms than is necessary or desirable. Its main deficiencies are as follows:

- Its scope is too limited because it does not apply to outsourced service providers to NSW government agenices.
- It does not make clear that disclosures of information purportedly authorised by superior officers, but not consistent with PPIP Act requirements, may be data breaches.
- It does not close a loophole in NSW privacy law where disclosures by employees outside the scope of their employment fall outside the PPIP Act's requirements, so agencies are not liable.
- The standard of liability for data breaches, 'likely to result in serious harm', is too narrow and too high.
- People outside an agency need to be able to trigger an investigation of a data breach.
- Both assessors of data breaches, and those carrying out internal reviews under the PPIP Act, should be able to come from outside the agency.
- The Privacy Commissioner should have the final say on whether affected individuals are informed of data breaches, not the agency concerned.
- The Commissioner should also have the final say on whether exemptions from requirements to notify individuals are applicable.

---

[1] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020* https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf

- Assessments to establish 'eligible data breaches' should be referred to an agency's internal Audit and Risk Committee, and established 'eligible data breaches' reported in the agency's Annual Report.
- A failure to give a data breach notification should result in a right for affected individuals to seek compensation for breach of PPIP Act. To make this right meaningful, there should be provision for statutory damages of $3,000 payable without need to prove actual damage, if a person's personal information is included in an eligible data breach.

A Table of all recommendations made is at the end of this submission.

## 1. Application to outsourced service provision

A principal deficiency of the draft Bill is that it does not apply to outsourced service provision on behalf of the NSW Government. The outsourcing of services traditionally provided by the government sector to the non-government sector, where the workforce can include both employees and volunteers, needs to be well managed to ensure protection for the personal information of service users and third parties such as community carers and family members including children.

In outsourcing service provision, it is incumbent upon the NSW government to ensure these NSW citizens have the same level of data protection for their personal information as those receiving services from government agencies, including the protections provided by the NSW MDBN scheme. It cannot be assumed that breaches by contracted organisations are covered by the NDB requirements of the *Privacy Act 1988 (Cth)*, because of the many exemptions from that Act's coverage, including in particular, the so-called 'small business exemption' for businesses with annual turnover under $3 million,[2] which exempts the majority of Australian businesses from liability.

The need to address the privacy obligations of such private sector entities or non-government organisations (NGOs) providing services on behalf of the NSW Government, is not a new issue:

a) The 2004 statutory review of the PPIP Act undertaken by the then Attorney General's Department recommended that the PPIP Act provide a structure for binding non-government organisations contracted by public sector agencies (Recommendation 13);[3]

b) The NSW Law Reform Commission in 2010 recommended that privacy protections be expanded where the NSW government outsources services under contract;[4]

---

[2] Office of the Australian Information Commissioner, *Part 4: Notifiable Data Breach (NDB) Scheme*
'The definition of APP entity generally does not include small business operators, registered political parties, state or territory authorities, or a prescribed instrumentality of a state (s 6C).'; 'Generally, SBOs do not have obligations under the APPs unless an exception applies (s 6D(4)).'

[3] NSW Attorney General's Department (2004) Review of the Privacy and Personal Information Protection Act, 1998. NSW Law Reform Commission (2010) "Report 127 – Protecting privacy in NSW," 30 – 36.

[4] NSW Law Reform Commission (2010) "Report 127 – Protecting Privacy in NSW," 30 – 36, st https://www.lawreform.justice.nsw.gov.au/Documents/Publications/Reports/Report-123.pdf

c) The survey of NSW NGOs undertaken for the 2015 review of the *Privacy and Personal Information Protection Act 1998* identified the need to strengthen the NSW privacy framework to address the uncertain obligations upon NGOs to achieve equivalent privacy protections for their service users;[5]

d) The Parliamentary Inquiry into service co-ordination for communities of high social need identified the need to address the privacy safeguards in the community sector.[6]

The PPIP Act is largely silent on the issue of contracted services other than for a 'person or body' that 'provides data services'[7] or in relation to retention and security of personal information.[8] There is not a line of authority from the NSW Civil and Administrative Tribunal (NCAT) decisions on the privacy obligations of the NSW public sector when contracting-out. The situation becomes more complex again when the contracted provider uses sub-contractors/agents.[9]

The 2015 review by the then Privacy Commissioner of the *Privacy and Personal Information Protection Act 1998,* recommended the PPIP Act be amended to clearly cover contracted service providers and contractors (Recommendation 4, page 21). More specifically, the 2016 review of the employer, employee, and agent information privacy responsibilities recommended amendments of both NSW privacy statutes (PPIP Act and HRIP Act) be based upon sections 36 and 37 of the Queensland *Information Privacy Act 2009* and section 95B of the *Federal Privacy Act 1988* to enable the public sector to choose to retain responsibility for any privacy contravening conduct of its contractors and subcontractors, or alternatively, to enter into contracts that make contractors and any subcontractors directly liable as if they are public sector agencies.

---

[5] Report of the NSW Privacy Commissioner under section 61B of the Privacy and Personal Information Protection Act 1998 (February 2015). https://www.ipc.nsw.gov.au/sites/default/files/file_manager/20150212_Privacy%20Commissioners%20Report_FINAL_low-res.pdf

[6] NSW Parliament, Standing Committee on Social Issues, (2015) Service co-ordination into communities of high social need.

[7] PPIPA s3, the definition of 'public sector agency' at (g) refers to 'a person or body' that receives funding from a public sector body to provide 'data services'. The provision of data services does not cover, for example, personal support services.

[8] Under s12(d) PPIPA, in relation to 'retention and security of personal information', when a public sector agency engages an agent (contractor) to whom it will give personal information, the agency must ensure that it does everything reasonably within its power to prevent unauthorised use or disclosure of the information. These obligations under s12(d) do not require the public sector agency to do everything within its power to mprotect the data the contractor will collect or create while performing the contract, nor to notify individuals if their data is breached and there are risks arisiing from this breach.

[9] NSW Privacy Commissioner (2016), *NSW Informational Privacy Rights: Employer, Employee, and Agent Responsibilities*, at https://www.parliament.nsw.gov.au/tp/files/70404/20-02-2017%20-%20NSW%20Informational%20Privacy%20Rights%20%20Legislative%20Scope%20and%20Interpretation.pdf

*Providing data breach notification protections against State governments*

The NSW Government Factsheet accompanying the draft Bill[10] does not mention those organisations and contractors providing services on behalf of the NSW Government and who collect extremely large amounts of personal information, and for whom it is acknowledged their systems and knowledge of compliance with data protection requirements for personal information is limited.[11] Moreover, the provisions of the draft Bill at Schedule 1, clauses [2], [3] and [4] relating to definition of "public sector agency" do not include contracted service providers. Nor does the proposed s. 59C(3).

The Bill therefore fails to address the obligations of contracted bodies, thereby establishing a two-class MDBN scheme for NSW citizens. NSW citizens have no choice over whether State government services are provided to them directly by agencies or indirectly through contracted service providers/agent. Further, in many cases they will be unaware of which type of entity is providing the service to them. In most cases, they have no choice about whether to provide personal information if they wish to obtain government services. Breaches will see the same risks and harms emerge regardless of the service provider.

For all these reasons, the right to equitable protection for those whose data is provided to contracted bodies needs the same notification rights as other NSW citizens. There is nothing these NSW citizens can do to mitigate the risks associated with an organisation not required to comply with privacy protection regulation. This lack of coverage will be found wanting by the public given that 71% of Australians believe small business should be covered by privacy legislation.[12]

The liability for ensuring that MDBN requirements are complied with should rest with the agency that has engaged the contracted service provider. It will then be up to the agency to ensure that its contractual arrangements are sufficient to ensure that it receives notifications of data breaches so that it can act accordingly under the MDBN scheme. The liability of contractors and agents under the scheme can be addressed by the same means.

There should not be any exemptions for agencies from this liability, and in particular no exemptions because contractors fail to inform agencies.

The over-riding principle should be that:

---

[10] Factsheet: "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." https://www.justice.nsw.gov.au/justicepolicy/Documents/proposed-changes-to-NSW-privacy-laws/privacy-and-personal-information-protection-amendment-bill-2021-factsheet.pdf

[11] Report of the NSW Privacy Commissioner under section 61B of the Privacy and Personal Information Protection Act 1998 (February 2015). https://www.ipc.nsw.gov.au/sites/default/files/file_manager/20150212_Privacy%20Commissioners%20Report_FINAL_low-res.pdf

[12] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020* https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf

1. all citizens whose personal information is provided to NSW agencies and/or their agents, are protected by the MDBN scheme, and

2. regardless of how agencies provide their services, that agencies have the responsibility for the consequences if that protection is not provided and data breaches occur.

**Recommendations**

1. *The Bill should be amended to explicitly ensure that an eligible data breach includes a data breach by contracted service providers or their agents.*

2. *The liability under the MDBN scheme for such a data breach should fall either: (i) Jointly upon the public sector agency and the contracted service provider/agent; or (ii) Solely upon the public sector agency (with any recovery by the agency being left to its contractual arrangements with the contracted service provider/agent). (Considerations of Commonwealth/ State relations may make (ii) the preferred approach.)*

## 2. Scope of 'eligible data breach'

The Bill states an 'eligible breach' requires both unauthorised access, disclosure and loss of information (s59C(1)(a)(i)) in combination with being 'likely to result in serious harm to an individual to whom the information relates'. Three issues are identified.

### 2.1. There is no definition of either 'authorised' or 'unauthorised'

It is known that officer(s) acting under instructions (ie purported 'authorisation') from CEOs/more senior managers provide personal information internally within their agency, externally to other public sector agencies, and to commercial entities, in contravention of the Information Protection Principles (IPPs) in NSW privacy legislation. This practice has been reported in evidence to the NSW Parliament.[13] The officers, so instructed, believed that they had been 'authorised'.

These supposed 'authorisations' should be prevented, and explicitly excluded from being 'authorisations' under the draft Bill, because they do not:

(i) override the IPPs in the *Privacy and Personal Information Protection Act 1998*;

(ii) guarantee protection against 'serious harm' to citizens, or

(iii) protect public officials against making a disclosure in contravention of the the PPIP Act.

---

[13] NSW Parliament, Committee on the Ombudsman, the Law Enforcement Conduct Commission and the Crime Commission, 'Review of the *Public Interest Disclosures Act 1994'*, Report 3/56 – October 2017 Report 3/56 2017 https://www.parliament.nsw.gov.au/ladocs/inquiries/2401/Report - Review of the Public Interest Disclosures Act 1994.PDF paras 1.44-1.45; Supplementary Submission (3A) of the NSW Privacy Commissioner to the Parliamentary Committee 2016 '*Review of the Public Interest Disclosures Act 1994* ' https://www.parliament.nsw.gov.au/ladocs/submissions/56447/Submission%203A%20-%20Office%20of%20the%20Privacy%20Commissioner.pdf; Report of the

Operational staff are both confused by and placed in 'no win' situations by such 'instructions / authorisations'. It has been a matter raised by the NSW Privacy Commissioner, by public sector unions covering clerical and health employees, and reportedly with public sector agencies.[14]

The appropriate safeguard against this possibility is for the terms of 'eligible data breach' to be couched in terms of 'access, disclosure and loss not in compliance with the IPPs' and removal of references to 'authorised'. Alternatively, 'authorised' could be defined so that it only refers to authorisations that comply strictly with the terms of the PPIP Act.

**Recommendations**

3. *The draft Bill should be a*mend*ed so that s.* 59C (1)(a)(i) *states* 'For the purposes of this Part, an eligible data breach means (a) both of the following are satisfied *(i) there are actions non-compliant with the IPPs that led to access, to, or unauthorised disclosure of, personal information, …'*

## 2.2. 'Non-work' loophole (employee 'frolics')

The effectiveness of this Bill as a protective mechanism for the privacy and data of NSW citizens depends upon not just on its provisions, but its interaction with the PPIP Act as it currently operates, including existing 'loopholes' in the PPIP Act.

A specific issue relates to mechanisms available to agencies to avoid liability for breaches of the PPIP Act. NSW privacy legislation does not define the terms 'employer', 'employee' and 'contractor', and relatedly, the distinction between where employer privacy responsibilities end and where they become the responsibilities of the employee (or agent) is not clear under the PPIP Act. This has facilitated NSW public sector agencies successfully arguing before the NSW Court of Appeal against responsibility for employees handling, for 'non-work purposes' of personal information ie 'use' (s17 PPIPA) and 'disclosure' (s18 PPIPA).[15]

Many areas of law regulating the responsibilities of government agencies and private service providers, include provisions requiring those organisations to have comprehensive systems in place for the protection of the rights of persons with whom they have dealings, for example tort, anti-discrimination, and workplace safety laws. Similarly, and additionally, laws and administrative systems also protect the property that organisations hold from corrupt exploitation by employees and their agents.[16]

---

[14] Ibid.

[15] *Director General, Department of Education and Training v MT* [2006] NSWCA 270 (NSW Court of Appeal)

[16] NSW Privacy Commissioner (2016), *NSW Informational Privacy Rights: Employer, Employee, and Agent Responsibilities*, at https://www.parliament.nsw.gov.au/tp/files/70404/20-02-2017%20-%20NSW%20Informational%20Privacy%20Rights%20%20Legislative%20Scope%20and%20Interpretation.pdf

The misuse of confidential information including personal information, has been a longstanding issue in Australian public sectors, and in NSW, the subject of an ICAC Inquiry.[17] Misuse of personal information is both a breach of privacy and a key enabler of corrupt conduct. Further, improper access to and disclosure of confidential information continues as a significant corruption risk particularly with the increasing value of personal information.[18] The requirements upon public sector agencies to be 'corruption resistant' includes the responsibility for ensuring employees are behaving correctly when in contact with personal information held by the agency, and for agencies to have systemic arrangements in place to manage and monitor access, use, loss and disclosure of personal information.

Members of the public have every right to expect that their personal information is not placed at risk by poor organisational practices including the failure to inculate lawful and appropriate handling of their personal information by agencies' employees and agents.

The draft Bill is an opportunity to do more to shift the focus to prevention of data breaches and their re-occurrences, by requiring agencies to have in place systemic data protection safeguards, as argued recently by the Queensland Crime and Corruption Commission.[19]

In the Bill as drafted, the concept of 'unauthorised' access, disclosure and loss of personal information not only enables agencies to avoid accountability for employees' conduct, but in combination with the loophole outlined, acts as a disincentive to agencies establishing adequate systems to inform, educate, train and refresh employees and contractors' capacity and capabilities for dealing lawfully with personal information held by the agency.

The Bill's current drafting favours organisational stances and operations of non-accountability for the handling of personal information, that is, if it can be said that the data breach arises from 'non-work' use and/or disclosure and/or loss of personal information (ie 'non-authorised'), then it is not the fault of the agency and its management. It is instead an employee acting on a 'frolic' even though this conduct concerns personal information held by the agency, and for which the agency has the responsibility to safeguard.

---

[17] Queensland Crime and Corruption Commission (2020) Operation Impala Report on misuse of confidential information in the Queensland public sector, February 2020 at https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-One-page-summary.pdf; NSW Independent Commission Against Corruption (1992) Report on Unauthorised Release of Government Information, Sydney, Vol 1.

[18] Queensland Crime and Corruption Commission (2020) Operation Impala Report on misuse of confidential information in the Queensland public sector, February 2020 at https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-One-page-summary.pdf

[19] Queensland Crime and Corruption Commission (2020) Operation Impala Report on misuse of confidential information in the Queensland public sector, February 2020 at https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-One-page-summary.pdf

*Providing data breach notification protections against State governments*

While it is valuable to have in place a MDBN mechanism to protect NSW citizens from harm following a data breach, the primary goal has to be upon prevention of such breaches occurring by the removal of such perverse incentives. This requires a clear responsibility placed upon agencies to have systems in place (as per NSW Auditor General reports) to safeguard their informational holdings.

In summary, legislative drafting that:

1. expands an existing loophole for agencies via inclusion of 'unauthorised access, disclosure or loss' enabling agencies to evade their responsibilities for NSW citizens' personal information,

and which

2. further entrenches the 'employee frolics' loophole, removes incentives from agencies to prevent data breaches occurring,

is not in the best interests of NSW citizens.

This Bill should make agencies responsible under the MDBN scheme irrespective of whether such 'employee frolics' occur. Such vicarious liability is what would be expected in the commercial world, and should also be the case with government.

**Recommendations**

4. *The PPIPA should be amended to allow victims of privacy breaches to have a right to complain against both a public sector agency and relevant employees. That is, the ability to request that the Tribunal make employees second respondents in cases where a public sector agency claims that its data security safeguards were adequate and that the agency should not be liable for the alleged conduct of its employees who contravened privacy laws. An agency should be responsible for making MDBN notifications irrespective of whether issues of unauthorised actions by employees are involved.*

## 2.3. Standard of eligibility: 'Likely to result in serious harm'

'Likely to result in serious harm' is a threshold too high, too narrow and too limiting. The Bill needs to be more cognisant of the threats to individuals' rights and freedoms. Informational privacy is a means to enjoy other rights such as non-discrimination, and the right to practise one's faith and beliefs. Conversely, the breach of informational privacy lessens and infringes not just the right to privacy but also other rights such as the non-discrimination, the right to practise one's faith and beliefs, and right to seek, receive and impart information and ideas.

The draft Bill seeks to establish that judgement of what is 'serious harm', and its occurrence, is at the discretion of the departmental head of the department responsible for the putative data breach (s59D(2)(b), largely via the assessment process (s59F(1)).

International research[20] has shown that perception and determination of 'serious harm' is not clear-cut. 'Serious harm' does not meet the expectations of NSW citizens specifically, indicated by the OAIC 2017 survey "Australian Community Attitudes to Privacy".[21] This showed that 95% of those surveyed believed that if a government agency lost their personal information, they should be told about it. This is consistent with the results of the 2020 survey, and moreover, with what Australians feel is a mis-use of their personal information. In other words, it seems Australians want to know about data breaches of their personal information irrespective of considerations of 'serious harm'.

The threshold of 'serious harm' is also not conducive to achieving the aims of the Bill. In a practical sense, what may not be seen as 'serious' to a typically white, older, male, CEO/senior public official may be experienced extremely differently by a woman seeking assistance with domestic violence for example, or by an individual of diverse gender or sexual orientation or characteristics, or by an indigenous person, or by any person from a disadvantaged background.

Non-compliant access or disclosure of personal information has been authoritatively linked to discrimination, harassment, humiliation which have had serious effects upon individuals not appreciated by those removed from the consequences.[22] A larger vision is required and sensitivity to different individual life experiences is necessary within this Bill if it is to meet the needs and expressed wishes of people across all walks of life in NSW.

The appropriate test to be applied is not whether a data breach is 'likely to result in serious harm' but something more like whether it is 'unlikely to result in a risk to rights or freedoms'.

The draft MDBN provisions are far less protective than the leading international standards in relation to the threshold requirements for a data breach report to be made:

1) The European Union's *General Data Protection Regulation* (GDPR) requires notification to be made 'unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons' (art. 33(1)). First, the onus of

---

[20] Submissions to and Report of the UN Special Rapporteur on the Right to Privacy, Professor Joseph Cannataci, A/HRC/40/63, Annex 2, incl. para 96, at https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf;

[21] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020* https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf, p36.

[22] *International:* Report of the UN Special Rapporteur on the Right to Privacy, Professor Joseph Cannataci, A/HRC/40/63, Annex 2, incl. para 96, at https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf;

*Australia:* The Queensland Crime and Corruption Commission (2020) "Breaches of personal information were found to have ongoing and long-lasting effects including stress, feelings of vulnerability, financial loss, and frustration with the difficulty of obtaining redress or adequate compensation. Queensland Crime and Corruption Commission (2020) Operation Impala Report on misuse of confidential information in the Queensland public sector February 2020 https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-One-page-summary.pdf

proof is reversed (risk must be shown to unlikely, or notice is required). Second, 'rights and freedoms' must be considered, not only 'harm', which would not normally have such a wide connotation. Third, only a 'risk' is needed, not a 'likelihood'. Fourth, there is no qualification of the circumstances by 'serious'.

2) The Council of Europe's 'modernised' data protection Convention (Convention 108+) provides that reports to a data protection authority must be made of 'those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects' (art. 7(2)). Recital 64 includes 'humiliation' as what may be regarded as 'serious'. Recital 66 notes that complementary notifications could be made where there is 'a significant risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage'. This Convention uses 'risk for the rights and freedoms' as its overall term, but qualifies it with 'significant', a more inclusive and appropriate standard than 'serious'.

**Recommendations**

*5.* The relevant standard included in the Bill at 59(1)(a)(ii) should be *that a breach is 'likely to result in a significant risk to the rights and freedoms of an individual to whom the information relates'. This is a moderate statement of the standard to be met, less restrictive than 'likely to result in serious harm'.*

*6.* In addition, in 59G (1) the 'factors for consideration' when a breach is assessed should include '(g) the potentially differential effect of the breach on individuals from diverse or underprivileged backgrounds'; and (ii) the reference to 'serious harm to an individual' should be replaced by 'a significant risk to the rights and freedoms of an individual'.

## 3. MDBN processes: Misplaced discretionary authority

There are many aspects of the MDBN processes in the Bill which provide too much leeway for the body responsible for the data access, disclosure or loss, the government agency, to determine such matters as:

(i) if a potential breach needs investigation;

(ii) if there is 'an eligible breach';

(iii) the investigatory process; and, most importantly,

(iv) whether individuals to whom the data relates, are to be advised of a risk to themselves (s59T; 59V; 59W).

These various steps in the process are now considered.

### 3.1. Triggering a possible breach investigation

The necessity to investigate a possible eligible data breach is triggered only when "an officer or employee of a public sector agency reasonably suspects that an eligible data breach has occurred" [s59D (1)].

This ignores the realities that:

a. Outsourcing and particularly of ICT services, requires recognition that those in contact with the agency in capacities other than as 'an officer' or 'employee', may be aware of possible data breaches not apparent to officers/ employees, or against the interests of these officers/employees to bring to the attention of the agency/senior officers;

b. It is also particularly likely that the reasonable suspicion of an 'eligible data breach' may be identified by the data subject as outlined in the legal matters and case studies recently reported by the Queensland Crime and Corruption Commission's following Operation Impala, including, as they identified, by women escaping domestic violence;[23]

c. It is also possible that the NSW Privacy Commissioner or another oversight body, for example, the NSW Ombudsman, or enforcement body such as NSW Police, following contact by a member of the public, may have reasonable suspicion and should be able to trigger an assessment by notifying and/or requiring the agency to assess the possibility of an eligible data breach. It has been shown that Australians are as equally likely to contact the Privacy Commissioner or Police or the organisation they think was involved with a mis-use of their personal information.[24]

The draft Bill needs provision for these eventualities. Any person who reasonably suspects that an eligible data breach has occurred should be able to report this to trigger an investigation or assessment.

### 3.2. Assessment of 'eligible data breach'

The assessment of whether there is an 'eligible data breach' needs to be seen in the context also of the process of internal review under the PPIP Act. It is possible that notification of an 'eligible data breach' will lead to requests for a PPIP Act internal review by the agency responsible.

Under the PPIP Act, Part 5, section 53(4) the person who can undertake an internal review is specified as *'an employee or officer of the agency'.* The statutory review of the

---

[23] Queensland Crime and Corruption Commission (2020) Operation Impala Report on misuse of confidential information in the Queensland public sector

February 2020 https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-One-page-summary.pdf

[24] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020* https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf, p8; p62.

PPIP Act undertaken by the Attorney General's Department in 2004 recommended that agencies should be able to outsource their internal review obligations to appropriately qualified agents (Recommendation 24) to provide greater flexibility, particularly for smaller agencies.

In contrast to the PPIP Act, it appears that under the draft Bill at s. 59F (2) (c), an 'assessor' of what is an 'eligible data breach' can be someone acting on behalf of the public sector agency the subject of the breach. It is inconsistent and questionable as to due process, if subsequent Internal Reviews under the PPIP Act have to be undertaken by an employee or officer of the agency subject of the breach.

Amendment of the PPIP Act to deal the removal of the restriction limiting who can carry out internal reviews, could be enabled by amendments included in the draft MDBN Bill.

### 3.3. Who should decide on notification to individuals?

The decision to notify individuals affected by an eligible data breach is made by the head of the agency (s. 59K), an official responsible to a Minister and therefore potentially subject to pressure from a political source, whether directly or indirectly.

In contrast to the draft Bill, other instruments, authorities and practices show that the Privacy Commissioner, not the agency head, is the appropriate authority to make such a decision:

- The NSW Law Reform Commission recommended an agency not be required to notify an affected individual where the Privacy Commissioner considers that notification would not be in the public interest or in the interests of the affected individual.[25]
- The NSW Fines Act 1996 s. 117C(2) provided a higher standard, in that it required the agency to notify the individual 'unless the Privacy Commissioner advises that notification is not appropriate in the circumstances' (see Endnote 1).
- The Queensland Crime and Corruption Commission (2020) proposed in their report at Recommendation 12 – Mandatory Notification Scheme that "….. the OIC be responsible for developing the scheme, and receiving and managing the notifications."[26]

[25] NSW Law Reform Commission Report 127 Protecting Privacy in New South Wales May 2010. At https://www.lawreform.justice.nsw.gov.au/Documents/Publications/Reports/Report-127.pdf

[26] Queensland Crime and Corruption Commission (2020) Operation Impala Report on misuse of confidential information in the Queensland public sector, p18

February 2020 https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-One-page-summary.pdf

*Providing data breach notification protections against State governments*

- The European Union's GDPR, the international standard of best practice, provides that the supervisory authority (the Privacy Commissioner) may require the agency to notify affected individuals of the breach (GDPR, art. 34(4)).[27]

- The Explanatory Report accompanying Council of Europe Convention 108+ provides that 'In cases where the controller does not spontaneously inform the data subject of the data breach, the supervisory authority, having considered the likely adverse effects of the breach, should be allowed to require the controller to do so. Notification to other relevant authorities such as those in charge of computer systems security may also be desirable. '[28]

The view of Australian citizens has been ascertained ie 95% want to be told of what has happened to their personal information.[29] Moreover, the requirement to notify individuals of eligible data breaches has been reported as providing an incentive to entities to ensure reasonable steps are in place to adequately secure personal information.[30]

It appears that the draft Bill is out-of-step with Australian and international opinion and practices on this point. It should be amended.

**Recommendations**

7. *Any person who reasonably suspects that an eligible data breach has occurred should be able to report it to trigger an investigation.*

8. *Introduce consistency between the section 59F (2) (c) of the draft Bill and the section 53 (4) (b) of the PPIP Act (internal review by agency) to enable agencies to establish that a person acting on behalf of the public sector agency, is able to undertake an internal review.*

9. *The public service head should consult the Privacy Commissioner on whether individuals to whom the data relates, are to be advised of a risk to themselves.*

10. *The Privacy Commissioner, not the agency, should make the decision whether an agency is not required to notify an affected individual because notification would not be in the interests of the affected individual, or for other reasons provided in the draft Bill.*

---

[27] GDPR, art. 34(4) : 'If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require that it do so…'

[28] Council of Europe *Convention 108 +Convention for the protection of individuals with regard to the processing of personal data,* Explanatory Report, Para. 66 https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

[29] The 2017 survey "Australian Community Attitudes to Privacy" OAIC. (Not reported in 2020 survey).

[30] QCCC, 2020 ibid: NSW Law Reform Commission https://www.lawreform.justice.nsw.gov.au/Documents/Publications/Reports/Report-123.pdf

11. *For greater clarity, 59M(1)(a) should be amended by replacement of 'notify each individual' with 'notify any or all individuals'. In addition, a new 59M(1)(c) should be added, stating 'If subsection (1)(a) applies to some affected individuals only, then (1)(b) shall apply to those individuals, and subsection (2) shall apply to all other affected individuals.*

## 3.4. Exemptions from obligations to notify

There are exemptions from obligations to notify affected individuals of data breaches in ss. 59R – 59W. The exemptions apply 'if the head of a public sector agency believes on reasonable grounds' that the conditions necessary for the exemption are satisfied.

Some of the conditions for exemptions in these sections are similar to those found in the EU's GDPR (art. 34(3)), but in the GDPR the final decision on whether these conditions are met lies with the supervisory body (ie the Privacy Commissioner) (GDPR, art. 34(4)), not with the agency head.

There are always dangers of conflicts of interest and bias where an agency has the power to exempt itself from statutory requirements which otherwise apply to it, particularly when such decisions potentially involve behaviour for which it could be censured, such as data breaches. Good practice is to minimise the possibility of such decision-making powers being abused.

These provisions in ss. 59R – 59W in the draft Bill contain very limited measures to prevent abuse, other than a requirement in some sections (only) to notify the Privacy Commissioner when an agency relies on an exemption. There are also, in some sections, requirements to consider time-limited exemptions, and to consider any Guidelines made by the Privacy Commissioner.

The preferable approach would be for the draft Bill to follow the GDPR as international best practice, and to give the Privacy Commissioner the final decision as to whether the conditions for exemption are met.

Some exemptions (s. 59S, s. 59T and s. 59U) do not contain a requirement that the Privacy Commissioner be informed of the use of the exception, whereas others do have such a notification requirement (s. 59V and s. 59W). There is no justification for failure to inform the Commissioner that such grounds have been used, and it would be impossible for the Commissioner to review the exercise of such grounds (as recommended above) unless they receive notice that such grounds have been utilised. This should be amended.

Some comments on specific provisions are also needed:

Concerning s. 59J, the ability of the Departmental/agency head to grant ongoing extension to his/her agency to extend the assessment process is not limited – the requirement to report to the Privacy Commissioner or to provide an interim report makes up for this deficit to a minor extent, as these requirements are substantive qualifications upon this potential loophole. Further, the extension of

time is not, at the minimum, in consultation with the Privacy Commissioner. Nor is there a limitation on the number of occasions of extensions possible.

The power for agency heads to exempt disclosures to affected individuals because they might 'worsen the agency's cyber-security' or 'lead to further data breaches' (s. 59W) is so broad ('cyber-security' is not defined) that it has obvious potential to be used by agencies to hide their own failures instead of remedying them.

- There is also no provision in s. 59T for, or requirement for re-consideration of this notification exemption, if it turns out that the mitigating actions have not prevented harms/risks to the rights and freedoms of the individual(s). This is in contrast to s. 59V(4) and s. 59W (4) and (5), which provide for a more qualified exemption leeway. There should be a requirement that exemptions made under s. 59T be reviewed after a period of time.

If the Privacy Commissioner has the final decision as to whether the conditions for exemption are met, then the dangers of these exemption procedures being misused will be reduced considerably. To achieve this, the Commissioner must receive notice when such grounds are utilised.

**Recommendations**

12. *In relation to ss. 59R – 59W in the draft Bill, the Privacy Commissioner should be given the final decision as to whether the conditions for exemption are met.*

13. *In relation to ss. 59S – 59U in the draft Bill, the Privacy Commissioner should be notified by an agency when that agency exercises the relevant exemption.*

14. *The drafting of 59L(3) allowing that the information requested at s. 59L(1) & (2), does not have to be provided if 'not reasonably practical for the information to be provided' requires tightening to ensure that it is not interpreted as negating the requirement to provide information to the Privacy Commissioner or to provide whatever information is available.*

15. *There should be a requirement that exemptions made under s. 59T be reviewed after a period of time.*

# 4. Consequences of breaches and notifications

Improving the informational privacy of NSW citizens requires more than notification to the Privacy Commissioner and affected individuals of data breaches. Any data breach may (or may not) indicate a breach of the security principle, or other principles, in the PPIP Act. Appropriate consequences should follow, and the draft Bill should include steps to ensure they are followed.

## 4.1. Governance processes

In relation to addressing the causes of the suspected/eligible breach, there is no attention in the Bill to preventing further breaches. That this is required is beyond doubt.[31] It has been found, for example, that Service NSW which handles the personal information of the NSW population on behalf of multiple agencies:

> "is not effectively handling personal customer and business information to ensure its privacy. It continues to use business processes that pose a risk to the privacy of personal information. ……. Previously identified risks and recommended solutions have not been implemented on a timely basis".
>
> NSW Auditor General December, 2020.[32]

To achieve this requires explicit linkages to internal accountability and governance mechanisms.

First, in response to any eligible data breach, agencies should be required to incorporate a Privacy by Design approach into executive decision-making processes, such as instituting systemic practices to monitor access to personal information databases, where this does not already occur.

Second, the Bill also does not specify, as it should for avoidance of doubt, that the assessment of any eligible data breach is referred to the entity's internal Audit and Risk Committee. While this may be a matter which could be included in the Privacy Commissioner's Guidelines, such an obvious step would be better included in the draft Bill, as a systemic practice to reduce the likelihood of re-occurrences of data breaches. The Bill is silent on the need to audit access to the personal information held either within one agency or across agencies in the case of shared personal information. This is of concern considering the significantly important role of access audits in the prevention and detection of improper conduct.

Third, all eligible data breaches should be publicly reported in agency Annual Reports. Public reporting of organisational performance is a valuable accountability mechanism. To increase accountability for management of personal information collected from NSW citizens the *Annual Reports Act 1984* and related Regulations should be amended to require reporting of eligible breaches and actions taken to address and prevent further breaches. The 'public register' specified in 59M(2) is insufficient, because the audience for temporary online provision of information is different from the audience for more permanent reference publications such as annual reports. Nor is this recommendation for inclusion in Annual reporting intended as a substitute for notification of affected individuals (by whichever means in 59M(2)). However, the public notification registers of agencies referenced at (59O(b) and s59ZD should be linked to and from the NSW Privacy Commissioner's website, as a further element of accountability.

---

[31] As established by NSW Auditor General reports of agencies of the information management practices of key agencies such as Births, Deaths and Marriages; Education; Health amongst others.

[32] New South Wales Auditor-General, *Service NSW's handling of personal information, Special Report* 18 December 2020. Viewed 30 June, 2021. Available at https://www.audit.nsw.gov.au/sites/default/files/documents/Final%20report%20-%20Service%20NSW%20s%20handling.pdf

*Providing data breach notification protections against State governments*

Although somewhat outside this Bill, it is worth noting that training specifically relating to informational privacy, the appropriate use of information systems and the MDBN scheme should be mandatory for all employees and agents/contractors dealing with personal information.

**Recommendations**

16. *Agencies should be required to incorporate a Privacy by Design approach in response to any eligible data breach.*
17. *The assessment of any eligible data breach should be required by the Bill to be referred to the entity's internal Audit and Risk Committee.*
18. *Agencies should be required to report in their Annual Report any 'eligible data breaches' under the MDBN scheme.*

## 4.2. Compensation for individuals aggrieved by breaches

The vast majority of Australians want the right to seek compensation in the courts for a breach of privacy (78%).[33]

The absence of civil remedies for serious invasions of privacy in Australia[34] makes it even more important that the NSW privacy legislation protects individuals and provides compensatory mechanisms for those who are adversely affected by any breaches of PIPPA, including by failures to comply with the MDBN requirements. Any appropriate legislative response should make provision for compensation or other reparation for individuals who have been aggrieved by such breaches.

The draft Bill does not provide that the failure of an agency to comply with any of 59L to 59P constitutes non-compliance with either the PPIP Act or the IPPs to which it prescribes adherence by agencies (s. 21), so that any person adversely affected is entitled to seek remedies under the PPIP Act.

---

[33] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020*, https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf

[34] The number of recommendations from Australia law reform and human rights bodies for the introduction of a statutory tort for misuse of private information continues to grow. The Queensland Crime and Corruption Commission has recommended that the Queensland Government consider the introduction of a statutory tort for serious invasion of privacy by the misuse of private information, such as by collecting or disclosing private information about the plaintiff.

Our recommendation is consistent with NSW LRC (2010) Recommendation 9.2: '(4) Data breach notification provisions should be enforced in the same manner as an IPP under the *Privacy and Personal Information Protection Act 1998* (NSW).'[35]

Ensuring that there is an action for compensation available is the first step, but it is not sufficient, because in cases of data breaches (or the breach of security principles that often accompany them), it is usually very difficult for plaintiffs to establish that they have suffered actual damage as a result of the breach(es). For this reason, in Korea's data privacy law, there are provisions for statutory damages of 3M Korean won (approx. US$3,000) to be paid to a person whose personal data has been included in a data breach, without need for them to prove actual damage, unless the data controller can prove that the data breach involved no negligence on their part. The *California Privacy Rights Act of 2020* also includes provision for statutory damages, limited to US $750 per consumer per incident (1798.150(a)).[36] We recommend that a similar approach should be taken in NSW.

**Recommendations**

19. *The draft Bill should provide that the failure of an agency to comply with any of 59L to 59P constitutes non-compliance with IPPs (s21PPIPA), so that any person adversely affected is entitled to seek remedies under PPIPA.*

20. *The draft Bill should provide for statutory damages of $3000 to be payable to any person whose personal data has been included in a data breach, without need for them to prove actual damage, unless the agency who is the data controller can prove that the data breach involved no negligence on its part.*

---

[35] NSW Law Reform Commission: Report 127 *Protecting Privacy in New South* Wales May 2010. At https://www.lawreform.justice.nsw.gov.au/Documents/Publications/Reports/Report-127.pdf

[36] G. Greenleaf ' California's CCPA 2.0: Does the US Finally Have a Data Privacy Act?' (2020) 168 *Privacy Laws & Business International Report*, 13-17, https://ssrn.com/abstract=3793435

## 5. **Table of** Recommendations

1. *The Bill should be amended to explicitly ensure that an eligible data breach includes a data breach by contracted service providers or their agents.*

2. *The liability under the MDBN scheme for such a data breach should fall either: (i) Jointly upon the public sector agency and the contracted service provider/agent; or (ii) Solely upon the public sector agency (with any recovery by the agency being left to its contractual arrangements with the contracted service provider/agent). (Considerations of Commonwealth/ State relations may make (ii) the preferred approach.)*

3. *The draft Bill should be amended so that s. 59C (1)(a)(i) states 'For the purposes of this Part, an eligible data breach means (a) both of the following are satisfied (i) there are actions non-compliant with the IPPs that led to access, to, or unauthorised disclosure of, personal information, …'*

4. *The PPIPA should be amended to allow victims of privacy breaches to have a right to complain against both a public sector agency and relevant employees. That is, the ability to request that the Tribunal make employees second respondents in cases where a public sector agency claims that its data security safeguards were adequate and that the agency should not be liable for the alleged conduct of its employees who contravened privacy laws. An agency should be responsible for making MDBN notifications irrespective of whether issues of unauthorised actions by employees are involved.*

5. *The relevant standard included in the Bill at 59(1)(a)(ii) should be that a breach is 'likely to result in a significant risk to the rights and freedoms of an individual to whom the information relates'. This is a moderate statement of the standard to be met, less restrictive than 'likely to result in serious harm'.*

6. *In addition, in 59G (1) the 'factors for consideration' when a breach is assessed should include '(g) the potentially differential effect of the breach on individuals from diverse or underprivileged backgrounds'; and (ii) the reference to 'serious harm to an individual' should be replaced by 'a significant risk to the rights and freedoms of an individual'.*

7. *Any person who reasonably suspects that an eligible data breach has occurred should be able to report it to trigger an investigation.*

8. *Introduce consistency between the section 59F (2) (c) of the draft Bill and the section 53 (4) (b) of the PPIP Act (internal review by agency) to enable agencies to establish that a person acting on behalf of the public sector agency, is able to undertake an internal review.*

9. *The public service head should consult the Privacy Commissioner on whether individuals to whom the data relates, are to be advised of a risk to themselves.*

*Providing data breach notification protections against State governments*

10. *The Privacy Commissioner, not the agency, should make the decision whether an agency is not required to notify an affected individual because notification would not be in the interests of the affected individual, or for other reasons provided in the draft Bill.*

11. *For greater clarity, 59M(1)(a) should be amended by replacement of 'notify each individual' with 'notify any or all individuals'. In addition, a new 59M(1)(c) should be added, stating 'If subsection (1)(a) applies to some affected individuals only, then (1)(b) shall apply to those individuals, and subsection (2) shall apply to all other affected individuals.*

12. *In relation to ss. 59R – 59W in the draft Bill, the Privacy Commissioner should be given the final decision as to whether the conditions for exemption are met.*

13. *In relation to ss. 59S – 59U in the draft Bill, the Privacy Commissioner should be notified by an agency when that agency exercises the relevant exemption.*

14. *The drafting of 59L(3) allowing that the information requested at s. 59L(1) & (2), does not have to be provided if 'not reasonably practical for the information to be provided' requires tightening to ensure that it is not interpreted as negating the requirement to provide information to the Privacy Commissioner or to provide whatever information is available.*

15. *There should be a requirement that exemptions made under s. 59T be reviewed after a period of time.*

16. *Agencies should be required to incorporate a Privacy by Design approach in response to any eligible data breach.*

17. *The assessment of any eligible data breach should be required by the Bill to be referred to the entity's internal Audit and Risk Committee.*

18. *Agencies should be required to report in their Annual Report any 'eligible data breaches' under the MDBN scheme.*

19. *The draft Bill should provide that the failure of an agency to comply with any of 59L to 59P constitutes non-compliance with IPPs (s21PPIPA), so that any person adversely affected is entitled to seek remedies under PPIPA.*

20. *The draft Bill should provide for statutory damages of $3000 to be payable to any person whose personal data has been included in a data breach, without need for them to prove actual damage, unless the agency who is the data controller can prove that the data breach involved no negligence on its part.*

## Endnotes:

### 1: *FINES ACT 1996 - SECT 117C* – Unlawful disclosure of personal information

117C Unlawful disclosure of personal information

(1) If the Commissioner becomes aware of an unlawful disclosure of personal information about an individual that is held by the Commissioner, the Commissioner must, within 28 days after becoming aware of the disclosure, notify the individual of that disclosure in accordance with any directions given to the Commissioner by the Privacy Commissioner in relation to the matter.

(2) However, the Commissioner is not required to notify the individual of the disclosure if the Privacy Commissioner advises that notification is not appropriate in the circumstances.
(3) The Privacy Commissioner is to include information about all unlawful disclosures under this section in the Privacy Commissioner's annual report for the period in which the disclosures occurred.
(4) In this section--
**"personal information"** has the same meaning as in the *Privacy and Personal Information Protection Act 1998* .