SalingerPrivacy

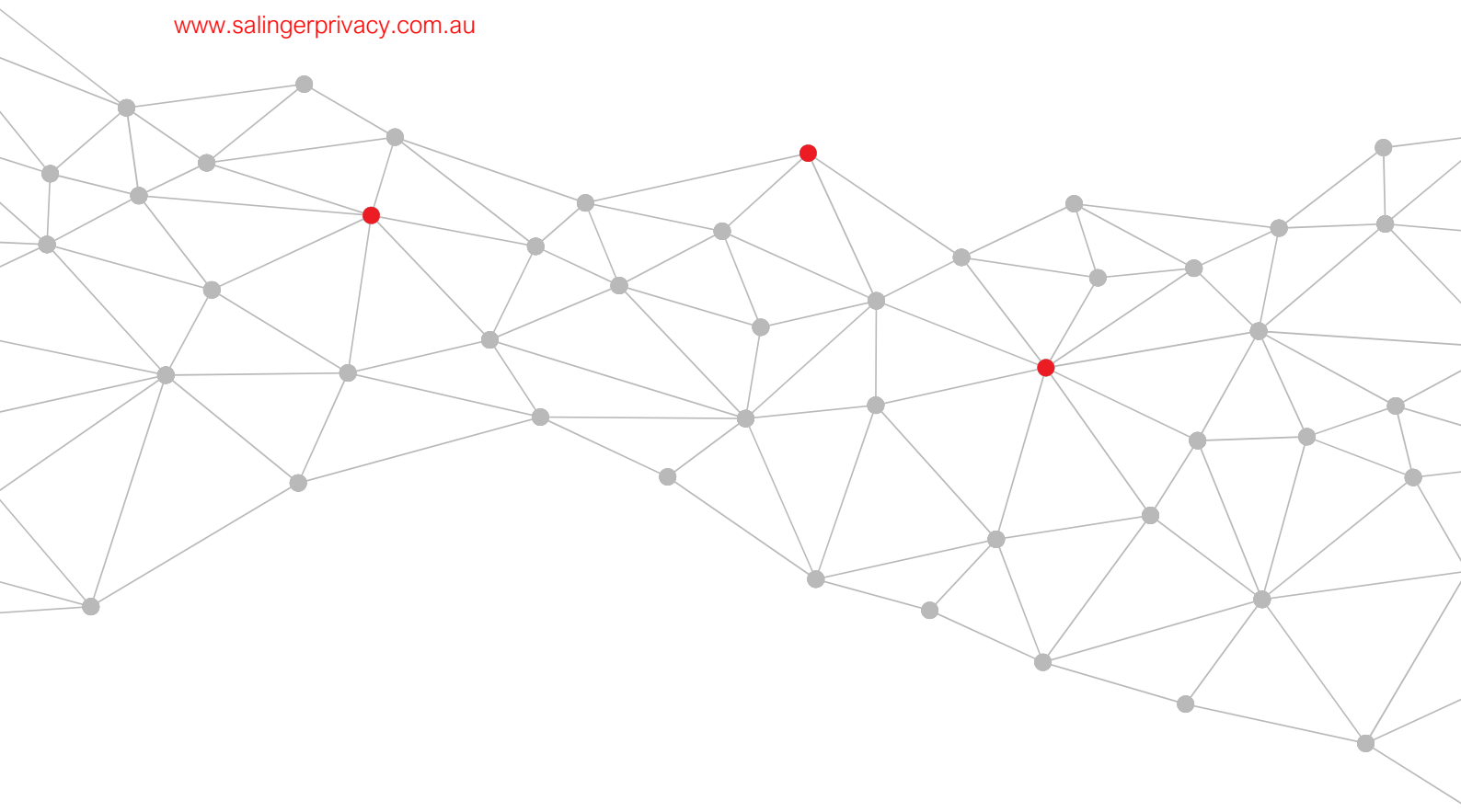
We know privacy inside and out.

Submission in relation to the Privacy and Personal Information Protection Amendment Bill 2021

NSW Department of Communities & Justice

13 June 2021

Salinger Consulting Pty Ltd
ABN 84 110 386 537
PO Box 1250, Manly NSW 1655
www.salingerprivacy.com.au



Covering letter

13 June 2021

NSW Dept of Communities & Justice
By email: policy@justice.nsw.gov.au

Dear Sir / Madam,

RE: The draft PPIP Amendment Bill

Thank you for the opportunity to make submissions in relation to the Public Consultation Draft of the Privacy and Personal Information Protection Amendment Bill 2021 (the Bill).

Please find our submission attached.

We have no objection to the publication of this submission.

Please do not hesitate to contact me if you would like clarification of any of these comments.

Anna Johnston
Principal | Salinger Privacy

Submission

I wish to begin by commending the general approach taken to introduce a mandatory notifiable data breach scheme in NSW, with respect to the objective of ensuring consistency with the federal notifiable data breach scheme under the *Privacy Act 1988* (Cth) (the Privacy Act).

This submission relates to concerns we have with the draft Bill, the first six of which appear to be unintended consequences:

1. The absence of a nexus between a data breach and an agency
2. The loophole created for contracted service providers, which will be covered by neither NSW nor federal scheme
3. An overly restrictive view of who may be harmed by a data breach
4. An overly restrictive time requirement on agencies for reporting
5. Notification requirements which go beyond what is necessary or useful
6. An information sharing exemption which is much too broad and could lead to significant harms in itself, and
7. The absence of any penalties or chances for meaningful enforcement of the scheme.

I will address these issues in turn.

1. The absence of a nexus between a data breach and an agency

There is no clear nexus between the realisation that an eligible data breach has occurred, and the requirement for a *particular* agency to respond under the Bill.

For example, if under s.59D an officer or employee of the Department of Education reasonably suspects that an eligible data breach has occurred at the Department of Customer Service, involving driver licence records held by the Department of Customer Service on behalf of Transport for NSW, which department is supposed to be responsible under the Bill: Education, Customer Service or Transport?

Is it the agency employing the person who found the breach, or the agency responsible for the breach, or the agency whose customers' personal information is at stake? The Bill does not actually assign responsibility for a breach with any causal nexus.

This example could be extended further: what if an employee of the Department of Education reasonably suspects that an eligible data breach has occurred at, say, a

Woolworths supermarket? Is this breach covered by this scheme? Without a casual nexus to suggest otherwise, at face value the Bill would suggest yes.

In our view, sections such as s.59D should refer to a data breach as involving or relating to personal information *held by* a particular public sector agency.

'Held by' is the formulation used in the federal Privacy Act, and in the PPIP Act in relation to the application of Information Protection Principles (IPPs) 5-12. Use of the 'held by' formulation would also be consistent with the existing protection for personal information being handled on behalf of a public sector agency by their contracted service provider; see s.4(4) of the PPIP Act.

2. The loophole created for contracted service providers, which will be covered by neither NSW nor federal scheme

It is not entirely clear, but from the phrasing of s.59C(3), it would appear that a data breach involving a contracted service provider to a public sector agency would *not* be regulated by the NSW scheme.

In our view this would be a significant weakness in the scheme, as contracted service providers to NSW public sector agencies are not regulated by the federal scheme either.

When private sector organisations are operating as a contracted service provider under a State contract, the practices involved in fulfilling that contract are exempt from both the Australian Privacy Principles (APPs), and the notifiable data breach scheme, under the federal Privacy Act.[1]

By way of example, a large consulting firm which assists their clients with data analytics capabilities would typically be bound by the APPs in the Privacy Act (and, by extension, the federal notifiable data breach scheme) because their turnover is more than $3M pa. However to the extent that their clients are NSW public sector agencies, which includes public universities and local councils as well as State government agencies, they will *not* be bound by the APPs – nor, by extension, will they be bound to the federal notifiable data breach scheme.

[1] The practices of a private sector organisation that are involved in fulfilling a 'State contract' (i.e. when operating as a contracted service provider to a State or Territory government) (see s.7B of the Privacy Act 1988) are not counted as an act or practice for the purposes of the APPs (see s.7(1)(ee) and s.15); and by extension, the notifiable data breach scheme also does not apply (s.26WE of the Privacy Act 1988). Nor can private sector contracted service providers 'opt back in' to the APPs (or the notifiable data breach scheme under the federal Privacy Act) even if they wanted to; the 'opt in to the APPs' method is only available for small businesses (s.6E), and the 'be prescribed in' method is only available for State and Territory instrumentalities (s.6F). Even if they agree to be bound by contract to meet a set of standards set by their client through the relevant set of State or Territory privacy principles, that contract is only enforceable by their client, providing no recourse or remedy for individuals who seek to complain about non-compliance with the standards set via that contract, and no investigative powers are triggered for the OAIC or any State or Territory privacy regulator.

Thus a data breach involving a private sector organisation which is handling personal information on behalf of a NSW public sector agency:

- Is certainly not regulated by the federal Privacy Act now, and
- May not be regulated by the NSW scheme without amendment to the Bill.

Not including data breaches which involve personal information being handled by contracted service providers to NSW public sector agencies would be a significant weakness in the NSW scheme.

We suggest that the Bill should be amended to:

- Include within scope any data breaches involving personal information that is being handled by contracted service providers to NSW public sector agencies, on behalf of those agencies; and
- Place primary responsibility for compliance with the scheme on the public sector agency (consistent with the way the IPPs already operate under the PPIP Act).

3. An overly restrictive view of who may be harmed by a data breach

The definition of an eligible data breach is made with reference to a test as to whether "an individual to whom the information relates" is likely to suffer serious harm from the breach (s.59C(1)(a)(ii)).

However third parties may also suffer harm from a data breach, and the definition should reflect this.

One example would be a data breach involving the unauthorised disclosure of information about the home address of a school student, which is used by the student's estranged father to track down and physically assault the student's mother. In this case the student themselves has not suffered the harm, though they are the individual 'to whom the information relates'.

Another example would be the unauthorised disclosure of genetic information about a patient, which led to harm to the patient's biological relatives.

We suggest that the definition should encompass if the breach "would be likely to result in serious harm to *any individual*".

4. An overly restrictive time requirement on agencies for reporting

Once an agency has conducted an assessment and determined that there has been an "eligible data breach", the head of the public sector agency "must, in the approved form, immediately notify the Privacy Commissioner" (s.59L(1)).

But what does 'immediately' mean in practice? Within one minute? One hour? One day?

In our view, the word 'immediately' should be defined, otherwise this will become a constant and distracting point of contention between agencies, affected individuals, the Privacy Commissioner and interested third parties such as the media.

We suggest instead a clearer definition, such as within 72 hours (the default timeframe for reporting data breaches under the GDPR), or 'as soon as practicable' (the formulation in the Privacy Act), or even something like "within one business day".

5. Notification requirements which go beyond what is necessary or useful

Under s.59M, the agency must notify *every* "individual to whom the personal information the subject of the breach relates".

In our view this is not necessary. The test for notification should be related to the same harm test as the definition of an eligible data breach.

In other words, if an agency is confident that some people whose personal information was involved in the breach are *not* likely to suffer serious harm, the agency should not be required to notify *those* individuals.

While in most cases the agency likely won't know who might suffer harm and who might not (in which case, notifying everybody affected is the sensible course of action), in some cases a distinction will be more obvious.

An example would be the unauthorised access by a rogue employee to the details of thousands of people holding driver licences. If the agency has already determined that the rogue employee was only interested in one of those people – his ex-wife for example, or a person on witness protection – then it could be the breach is likely to result in serious harm to just that one person. There should be no requirement to notify every Jane Smith whose records the rogue employee trawled while looking for the *particular* Jane Smith he was after.

6. An information sharing exemption which is much too broad and could lead to significant harms in itself

I am particularly concerned about s.59Q, which creates a new and overly broad exemption from compliance with the IPPs, ostensibly in pursuit of (though not in practice limited to) notification under this part of the PPIP Act. This power could be easily misused for widespread data collection beyond the purposes of this scheme.

Section 59Q allows public sector agencies to exchange the name and contact details, date of birth and (if relevant) date of death of "an notifiable individual". What is in scope here is set by s.59M, which as noted above currently covers *every* individual whose personal information was caught up in a data breach.

Section 59Q is not currently limited to individuals who need to be notified because they are likely to suffer serious harm. Nor does it require that the sharing of personal information be necessary *in order to notify the individual*; only that it is "reasonably necessary for the purposes of confirming the name and contact details…".

Since s.59Q creates a blanket exemption from the IPPs, it voids the requirement on those public sector agencies to take reasonable steps to protect the data security of the information being exchanged (IPP 5); or the requirement to not collect personal information that is overly intrusive (IPP 4); or the requirement to not use that personal information for any other purpose (IPP 10).

Section 59Q as drafted could also allow for 'information washing' following a data breach. A data breach could suddenly provide one agency the excuse to go on a widescale data collection or data cleansing operation, which would not otherwise be allowed. For example, an agency could seek to discover (from another agency) the name, contact details and date of birth of someone who has only ever corresponded with that agency by email.

In our view, s.59Q as drafted is unnecessary and unwise.

Instead, there could be a much more focussed exemption, as follows:

- The exemption should only relate to IPP 2 (prohibition on indirect collection) and IPP 11 (prohibition on disclosure)
- The exemption should only be in relation to individuals who are likely to suffer serious harm
- The exemption should only be triggered on the written approval of the Privacy Commissioner
- The Privacy Commissioner must first be satisfied that there is no practical alternative to effect notification of the data breach on individuals who are likely to suffer serious harm as a result of the data breach, and

- The exemption should prohibit the use of any personal information collected under this provision for any purpose other than to effect notification about the data breach; for example, the recipient agency should be prohibited from updating its records.

7. The absence of any penalties or chances for meaningful enforcement of the scheme.

Under this Bill, unlike under the federal Privacy Act, there is no fine or other penalty which can be levied on a public sector agency which fails to comply with the notifiable data breach scheme.

This scheme does not even allow for affected individuals to bring a case before the NSW Civil and Administrative Tribunal (NCAT) if an agency breaches these requirements, unlike if a complainant alleges a breach of the IPPs.

To be compensated for harm suffered as a result of a data breach, an affected individual would need to first demonstrate that the data breach was a result of a failure of the agency to take reasonable steps to protect data security – i.e. a breach of IPP 5. Asking individuals outside an agency to demonstrate systemic failures inside an agency is unfair. Further, when data breaches are the result of a 'rogue' employee, agencies often successfully argue that they are not liable for that conduct.

However even worse, under this notifiable data breach scheme, if an individual suffers harm because of the failure of the responsible agency to notify them in a timely fashion (such that the individual could otherwise have taken steps to prevent or mitigate the harm, which is the very point of a notification scheme), their recourse to compensation under this Bill is – nothing.

I suggest that the failure of an agency to comply with its assessment and notification obligations under this notifiable data breach scheme should be conduct which can be reviewed by NCAT, and for which an individual can seek compensation for any harm suffered.

At the very least, the failure of an agency to comply with its assessment and notification obligations under this notifiable data breach scheme should be defined as a "violation of, or interference with, the privacy of an individual" for the purposes of s.45 of the PPIP Act, such that an individual can make a complaint to the Privacy Commissioner and seek conciliation. This would be consistent with the federal Privacy Act's notifiable data breach scheme.

However we also note that the NSW Information & Privacy Commission is under-resourced in relation to its privacy function, and so the chances are low of agencies suffering robust investigation or being named in Parliament as in breach of the notifiable data breach scheme.

About the author

This submission was prepared by Anna Johnston, Principal, Salinger Privacy.

Anna has served as:

- Deputy Privacy Commissioner of NSW
- Chair of the Australian Privacy Foundation, and member of its International Committee
- a founding member and Board Member of the International Association of Privacy Professionals (IAPP), Australia & New Zealand
- a member of the Advisory Board for the EU's STAR project to develop training on behalf of European Data Protection Authorities
- a Visiting Scholar at the Research Group on Law, Science, Technology and Society of the Faculty of Law and Criminology of the Vrije Universiteit Brussel
- a Member of the Asian Privacy Scholars Network
- a member of the Australian Law Reform Commission's Advisory Committee for the Inquiry into Serious Invasions of Privacy, and expert advisory group on health privacy, and
- an editorial board member of both the Privacy Law Bulletin and the Privacy Law & Policy Reporter.

Anna has been called upon to provide expert testimony to the European Commission as well as various Parliamentary inquiries and the Productivity Commission, spoken at numerous conferences, and is regularly asked to comment on privacy issues in the media. In 2018 she was recognised as an industry leader by the IAPP with the global designation of Fellow of Information Privacy (FIP).

Anna holds a first class honours degree in Law, a Masters of Public Policy with honours, a Graduate Certificate in Management, a Graduate Diploma of Legal Practice, and a Bachelor of Arts. She was admitted as a Solicitor of the Supreme Court of NSW in 1996. She is a Certified Information Privacy Professional, Europe (CIPP/E), and a Certified Information Privacy Manager (CIPM).

About Salinger Privacy

Established in 2004, Salinger Privacy offers privacy consulting services, specialist resources and training.

Our clients come from government, the non-profit sector and businesses across Australia. No matter what sector you are in, we believe that privacy protection is essential for your reputation. In everything we do, we aim to demystify privacy law, and offer pragmatic solutions – to help you ensure regulatory compliance, and maintain the trust of your customers.

Salinger Privacy offers specialist consulting services on privacy and data governance matters, including Privacy Impact Assessments and privacy audits, and the development of privacy-related policies and procedures. Salinger Privacy also offers a range of privacy guidance publications, eLearning and face-to-face compliance training options, and Privacy Tools such as templates and checklists.

Qualifications

The comments in this submission do not constitute legal advice, and should not be construed or relied upon as legal advice by any party. Legal professional privilege does not apply to this submission.

SalingerPrivacy

We know privacy inside and out.

Salinger Consulting Pty Ltd
ABN 84 110 386 537
PO Box 1250, Manly NSW 1655
www.salingerprivacy.com.au