Comments on discussion paper – Mandatory notification of data breaches by NSW public sector agencies

General comments:

Would a state-based scheme work alongside, or instead of the Commonwealth scheme?

State-owned Corporations (SOC) fall outside of the definition of the public sector agency in the PPIP Act. Will a SOC also fall outside the definition of the mandatory data breach scheme? IPC guidance on data breaches to date state that the SOC are encouraged to notify the IPC of a breach (Sect 1.7.1)

Most agencies are not averse to the concept of mandatory notification of serious privacy breaches provided there are clear and concise, definitions and guidelines set down by the NSW Privacy Commissioner.

Question 1 –

Should the NSW Government introduce a mandatory data breach notification scheme for NSW public sector agencies?

We would support the introduction of a mandatory scheme for the following reasons:

- Removes current voluntary obligations
- Generates a focus on data breaches
- Places an emphasis on the need to notify the affected individual
- Appears to meet community expectations

The use of the term 'NSW public sector agencies' as defined by the *Privacy and Personal Information Protection Act 1998* (PPIP Act) does exclude State-Owned Corporations (SOC).

It would be useful for SOCs to be defined as public sector agencies for the purposes of the PPIP Act and Health Records and Information Privacy Act 2002 to assist with obligations and be captured in terms of reporting data breaches.

Question 2 –

Should legislation require NSW public sector agencies to report breaches:

(a) Where unauthorised access to or disclosure of personal information has occurred?

We feel that the focus on unauthorised access to or disclosure of personal information to be suitable because:

- These principles represent a consistent approach to the Commonwealth Scheme
- Will make it easier for practitioners to implement
- Factors in both internally and externally identified breaches

(b) Where any breach of an Information Protection Principle has occurred?

Broadening the scheme to include all principles could:

- Overburden agencies and the regulator
- Create a negative view of the Government
- Duplicate the effort agencies have due to the notification prompting affected individuals to complain
- It would not be conducive in the current environment

Question 3 -

(a) Is the threshold of 'likely to result in serious harm' appropriate, or should a different standard be applied?

Utilising the threshold 'likely to result in serious harm' is a suitable standard for the following reasons:

- It is consistent with the Commonwealth Scheme definition
- It provides a level of flexibility for agencies to consider when determining the breach severity
- It recognises that not all data breaches are likely to result in the level of risk necessary to notify individuals and the regulator

(b) Should legislation define the term serious harm?

We feel that a definition of serious harm may be challenging to reach due to the variability of a breach and the potential harm it could cause to individuals.

Using the different topics to consider (financial, reputational, physical, etc) are useful for agencies to factor in their assessments

Where possible, associating examples or methods to calculate serious harm will assist agencies in determining whether its breach constitutes 'serious harm'.

(c) Should legislation prescribe the factors an agency must consider when assessing whether a data breach meets the threshold of serious harm?

Yes, there should be an eligibility criteria assessment similar to the commonwealth scheme to assist with clarity and certainty of legislative guidance.

Question 4 -

Should legislation require NSW public sector agencies to report data breaches only where the agency has been unable to prevent likely risk of serious harm with remedial action?

We believe that only needing to report once the serious harm has been assessed, and remedial action has not reduced the harm to an acceptable level due to the following considerations:

- There's a risk of overreporting if triaging does not occur
- It allows agencies to test and respond to individual breaches as they arise
- It limits the exposure of agencies and the Government
- It doesn't create a scheme that produces a hysterical response from the community
- It focusses attention to those breaches that require attention

It would also reduce the unnecessary distress to the individual concerned and minimise the administrative burden on agencies to align with the Commonwealth Scheme.

Question 5 –

(a) What information should be notified to the NSW Privacy Commissioner and affected individuals in relation to data breaches?

We support drawing on the existing requirements under the voluntary scheme in NSW as well as the Commonwealth Scheme

(b) Should the legislation prescribe the form and content of the notification?

We would like the legislation to guide practitioner's responses for the benefit of the regulator and affected individuals. The legislation should clarify a distinction between notification to the Privacy Commissioner and what should be notified to the individual as both parties would not benefit from receiving the technical details of a data breach.

Question 6 –

What notification timeframe should be prescribed in the legislation?

We support the introduction of a timeframe consistent with the Commonwealth model as it:

- Provides consistency in application
- Doesn't require an immediate response when one may be challenging to provide
- Allows agencies some flexibility in reporting, should they be in a position to report earlier
- Some consideration should be given to mentioning the requirements of notifying the NSW Govt Cyber Security Office, should the incident arise out of cyber incident impacting data breach.

Question 7 –

(a) Does the NSW Privacy Commissioner require any additional powers to encourage compliance with a mandatory notification scheme?

The Privacy Commissioner already has expansive powers under s36 of the *Privacy and Personal Information Protection Act 1998* which could ensure the compliance with the scheme is met through the following:

- It ensures that agencies will take the introduction of the scheme seriously
- The Privacy Commissioner use the powers that may be necessary in the event that an agency is failing to provide a suitable response

(b) Should monetary penalties apply where NSW public sector agencies fail to comply with the requirements of the scheme?

We do not believe that monetary fines will be effective as the IPC is regulating other NSW government entities. Any fines are paid for out of NSW Government monies. The scheme should contemplate other regulatory tools such as mandatory publication of breaches and non compliance.

The introduction of penalties may:

- Encourage agencies to be more prepared to respond to breaches
- Could be used in the event of a serious breach as a precedent

Question 8 –

What exemptions from the requirement to notify individuals and the NSW Privacy Commissioner of eligible data breaches should apply?

Exemptions on the ground of jeopardising or prejudicing law enforcement activities seems reasonable. However, instead of blanket exemptions, perhaps the need to report extends only to the Commissioner, not to those individuals affected.

Other exemptions may apply if the agency believes that the notification of the breach to an affected individual may trigger an unhealthy response, if the individual is at risk of harming themselves, as an example. However, in that instance, the scheme should still require the agency to notify the Commissioner

Thank you for the opportunity to comment on discussion paper – Mandatory notification of data breaches by NSW public sector agencies.

Please accept this submission on behalf of the Consultative Committee for the NSW Right to Information and Privacy Practitioners Network.