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

General comments:

How does the Government wish to define data under the scheme? Is it in a written/documented form? The definition of personal information extends to information that may not be in written form (sect 4 PPIP Act). I think sometimes the terminology needs to be clarified.

Would a state-based scheme work alongside, or instead of the Commonwealth scheme? How would a NSW public sector agency manage a third party breach of its data, if the third party is subject to 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)

Question 1 –

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

Introducing a mandatory scheme would provide certainty for NSW public sector agencies as to whether to notify the regulator and affected individuals of a data breach. The current opt-in arrangement is ambiguous, lacks discipline and oversight. The introduction of a mandatory scheme would provide the regulator with a clearer picture of the extent of eligible breaches occurring, and making it better placed to deal with breaches and the reasons they occur.

NSW public sector agencies may already be notifying under existing arrangements when a breach results in a complaint and initiation of the Privacy Commissioner's internal review process.

The current legislative landscape sees NSW public sector agencies responsible for notification under the C'th NDB Scheme if the breach is to do with Tax File Number (TFN) Information. NSW public sector agencies may also be affected more broadly by the NDB Scheme if a third-party provider covered by the scheme has an eligible data breach while delivering services to that agency.

The scheme could be seen as an extension of current incident management practices within NSW public sector agencies.

The Community Attitudes to Privacy Survey 2017 would indicate that there is strong support from the public to be informed of data breaches. A scheme would also promote transparency and the opportunity for those affected to take appropriate steps to address any concerns that their personal information has been compromised.

The use of the term 'NSW public sector agencies' as defined by the PPIP Act does exclude State-Owned Corporations (SOC)

Question 2 –

Should legislation require NSW public sector agencies to report breaches:

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

Using the definition of a breach to include unauthorised access to or disclosure of personal information would be consistent with the NDB Scheme that already applies to NSW public sector agencies. The consistency of definition across multiple jurisdictions would produce useful statistics to benefit analysis, yield long-term trends and would make it easier for the community to understand.

From a practitioner's point of view, having a common understanding of what constitutes a breach simplifies the process of identification and promotion in the workplace. It could also help agencies articulate reporting requirements to third parties that they enter into contracts and agreements with, as well as the third parties implementing the scheme/s within their operations.

The unauthorised access principle (IPP/HPP 5) and the disclosure principles (IPP/HPP 11, HPP 12 and 13) could produce both internally and externally identified breaches.

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

To broaden the definition of a breach to include all the information protection principles could potentially introduce far more reporting. This could lead to a scheme that is resource heavy and may fail to meet objectives.

It would be interesting to look into the complaint statistics of the IPC and the OAIC, as well as the results of the Community Attitudes to Privacy Survey to determine whether there are other principles (apart from the access and disclosure principles) that commonly trigger complaints/reviews or could be in the public's interest to report on.

An individual currently has the ability to complain to an agency and the IPC about an agency's adherence to the IPPs/HPPs. However, whether they are informed by an agency that their information has been compromised is not defined by the principles or guidance from the IPC

Question 3 -

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

As a threshold, the likelihood of serious harm occurring seems more than appropriate. Whether there is a slightly lower threshold would require some further analysis. A member of the community may expect to be made aware on each occasion their personal information is breached. However, this could lead to an influx of reporting.

However the scheme defines the level of harm, it must do so with clear guidance to ensure that there is as little ambiguity as possible for agencies and practitioners. Using factors such as the type of information compromised, the quantity, its context and the risk to an individual and the agency that feature in the IPC's guidance are all helpful, however from an agency's point of view, it may apply all of those factors to its operation/function and then the decision about whether to report or not. A healthcare provider may have a different point of view to a regulator agency, as an example.

Consistency, where possible should be the better option, as it reduces any need to attempt to interpret the seriousness of harm.

(b) Should legislation define the term serious harm?

It may be challenging to come to a conclusive definition of serious harm if you were to attempt to cover this across the many functions that NSW public sector agencies represent. For example, if the scheme were to lean towards an individual's health information being breached as a higher level than an individual's contact information, those agencies holding health information may be further affected by the scheme.

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

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?

Having a threshold to assess against and then determine whether to report does seem reasonable. Agencies will find the reporting of all data breaches an onerous (and possibly trivial) activity, and could dilute the importance of the scheme when actual responses are called for (i.e. when they've been unable to prevent the risk of serious harm). Reporting all breaches would almost surely over burden the regulator.

It's interesting to draw on the results of the Community Attitudes to Privacy survey result highlighted in the discussion paper that states 95% of the community expect to be informed about when their personal information has been lost by a government agency.

A breach may still be in the public or regulator's interest if it exposes a failing of the NSW public sector agency to foresee or protect itself from a data breach. There may be additional reporting requirements for a NSW public sector agency to meet if the breach is a result of a malicious attack (to the NSW Government's Chief Information Security Office), which could result in reports in the media.

Perhaps the way around this is for there to be an annual reporting requirement for each agency. Published in the annual report along with commentary about the application of

NSW privacy laws, the requirement could be as simple as data breaches reported to the regulator; other data breaches.

However, introducing any type of reporting may set-up an agency as an unintended target for malicious actors interested in carrying out attacks.

Question 5 –

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

The information should be sufficient enough for the regulator to understand what has occurred and to give adequate assurance that measures are being/have been put in place to stop the breach from occurring, and then lessen the risk of harm to those affected.

For an individual that has been affected by the breach, the information should attempt to address similar objectives of providing sufficient information for the individual to know how to respond.

At a minimum, the information should contain:

- Information about the breach, including the nature of the breach, when it occurred, when it was discovered
- What information was compromised
- Whether the information is likely to be recoverable
- What steps the agency has taken to address the risk to individuals
- Information about how to contact the agency for further details
- Information about the rights the individual has to complain to the NSW privacy commissioner

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

The legislation should outline sufficiently the information that is required by the regulator in order to understand the breach and respond to the notification. This will need to be in some level of detail so that the agency can prepare the information once, rather than through multiple attempts to confirm the incident.

Agencies will have different methods of responding to incidents such as this and will likely be capturing a lot of information as a result. However, they may be hesitant to provide too much detail for reasons relating to its reputation, the level of understanding about the breach and other matters.

If the legislation were to prescribe the content, then it would be useful to work with established items in the Commonwealth model.

Question 6 –

What notification timeframe should be prescribed in the legislation?

The timeframe for the NDB scheme seems reasonable. It takes into account the ability to assess the breach and how it may affect individuals. This could be challenging if a breach has occurred and the nature of it is difficult to ascertain (consider malicious attack). Being provided with adequate time to investigate allows for a more considered approach to make assessments about the level of harm to an individual the breach may result in. The timeframe also allows for an agency to make a report earlier if there is clear evidence to suggest that the breach meets the scheme's reporting criteria.

Question 7 –

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

The NSW Privacy Commissioner may benefit from increased powers to ensure that compliance with the scheme is met. The C'th Commissioner's ability to pursue agencies using the interference of privacy requirements does send a strong message on the expectations of adherence and cooperation with the scheme. Another category to include could cover the inability of an agency to prevent a known breach from continuing.

The investigative powers that the NSW Privacy Commissioner currently has for complaints under Sect 45 of the PPIP Act could accommodate complaints in respect to non-compliance with the scheme.

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

Monetary penalties do attract the attention of agencies, the public and the media. So it may be acceptable to introduce such measures with the scheme. Utilisation of the penalties would also send a clear message about the expectations of agencies to comply with the scheme and take breaches of this nature seriously. However, I suspect that the preferred method of handling non-compliance with the scheme would be through a similar method outlined in 4.27 of the discussion paper.

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.