YoungmanConsultancy

[redacted]

Mandatory Notification of Data Breaches by NSW Public Sector Agencies
Policy, Reform and Legislation
NSW Department of Communities and Justice
GPO Box 31
Sydney NSW 2001

Compulsory reporting of data breaches

Dear Sir/Madam

I have read your Discussion Paper and I wish to make the following observations:

[redacted]

In regard to the issues you raise in your Discussion Paper:

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

Yes, I worked for the [redacted] for nearly 45 years and I have never found any form of self-regulation to work in the long term. At some point self-preservation or self-interest wins out and the organisation decides in its own best interests, as seen by the decision maker.

The fact that the instances of data breaches increased by 712% when reporting to the Australian Information Commissioner became mandatory demonstrates my point.

I think it is not in the best interests of the Government, the agencies or the general public to allow data breaches to remain unreported.

As you stated the general public expect such breaches to be made public.

Advising data breaches actually allows the Privacy Commissioner to be aware of the circumstances and better able to answer enquires it receives from the general public once it becomes general knowledge. It actually assists the process of dealing with enquiries.

2. Should legislation require NSW public sector agencies to report breaches:

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

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

Not necessarily, where the unauthorised access or disclosure involves only one person, the agency should have to notify him/her what information is involved, how the incident occurred and what action is being taken to correct the situation and deal with the offender.

In some cases, these matters are drawn to the attention of the agency by the individual to whom the information relates. In such cases, the matter is investigated, and the Privacy Commissioner is notified of the complaint, the outcome of the investigation and the result arising from the investigation.

I think this is still sufficient and a practical and reasonable solution to the mater. If the breach is detected by the agency, it should investigate the matter along similar lines to a Privacy complaint and notify the affected individual and the Privacy Commissioner within, say, 60 days. The time allowed under the Privacy Act to finalise Privacy complaints.

However, if the breach involves multiple records, i.e. more than one individual, then the agency should be required to report the breach.

3.

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

b) Should legislation define the term serious harm?

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

I think it is reasonable to define the potential damage by the term "serious harm". To refer to the damage as merely harm, risks agencies having to report every incident, even the ones where the agency may have identified it and be dealing with it already, e.g. the case of a Privacy complaint.

I don't think the term should be defined within the Act. There is a similar reference in the Table in Section 14 of the GIPA Act:

> *3 Individual rights, judicial processes and natural justice There is a public interest consideration against disclosure of information if disclosure of the information could reasonably be expected to have one or more of the following effects:*

> *(f) expose a person to a risk of harm or of serious harassment or serious intimidation.*

The meaning of the term has been examined numerous times in appeals to NCAT and the previous ADT.
In ***AEZ v Commissioner of Police, NSW Police Force [2013]*** *NSWADT 90* Judicial Member Molony stated, in part:

> *"Harm is a concept frequently used by the law. The criminal law prohibits assaults occasioning bodily harm. This has been interpreted in its ordinary meaning to" include any hurt or injury calculated to interfere with the health or comfort of [the injured person]": see* ***R v Donovan [1934]*** *2KB 498. "Serious harm" is a concept used in criminal defamation, which requires proof of an intent to cause serious harms. Section 40 of the Civil Law (Wrongs) Act 2002 (ACT) on the other hand defines "harm" to be harm of any kind, including personal injury, damage to property and economic loss. Harm is also a concept in child protection: in section 9 of the Child Protection Act 1999 (Qld) it is defined as "as any detrimental effect of a significant nature on the child's physical, psychological or emotional wellbeing."*
>
> *In the context of s 14 of the GIPA Act I am inclined to the view the meaning of harm should be confined to a real and substantial detrimental effect on a person, rather than on their business interests. This is so given the juxtaposition of the word "harm" with the concepts of serious harm and intimidation, and the fact that economic and business interests are the subject of public interest consideration against disclosure in part 4 of the section 14 Table. A detrimental effect may be to a person's physical, psychological or emotional wellbeing."*

I believe the definition should arise from case law and, therefore, be able to reflect legal opinion as in evolves. If it is placed within the legislation and there is a view at a later date, that it needs to be revised, it creates an unnecessary legislative burden.

On the other hand, examples of when matters should be reported may be beneficial. As long as it doesn't allow agencies to down-play situations in order to avoid having to notify them.

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?**

No, again it provides an opportunity for agencies to excuse the situation an avoid having to report it.

Part of the role of the Privacy Commissioner could be to suggest actions that may either be best practices in other jurisdictions or have worked in other agencies. Improving the ability of agencies to better protect the data they hold.

The main point is that the Privacy Commissioner and agencies try to work together as allies to deal with these issues, rather than enemies.

The suggestions in the Discussion Paper would resolve the issue, but it is preferable that the agency can work with the Privacy Commissioner to try and avoid similar problems in the future.

5.

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

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

The proposals list under Sections 4.16 to 4.19 seem a reasonable approach.

Question 6:
What notification timeframe should be prescribed in the legislation?

There should be no reason why the data breach could not be reported without undue delay and, in any case, within 5 working days. This doesn't mean the agency cannot still investigate the situation and report back to the Privacy Commissioner as to the findings of the investigation, the remedial action proposed and future preventative steps to be taken.

A decision about the need to go public or notify the people affected by the breach can be resolved through discussions between the Privacy Commissioner and the agency.

7:

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

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

The current powers appear suitable, as far as they go. However, there does need to be the ability to deal with situations where an agency or an individual within an agency intentionally fails to report a breach in order to protect their or another staff member's actions. The relevant provisions of the Commonwealth legislation appear to be reasonable.

Question 8:

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

It is reasonable that where the data is held by two agencies, only one needs to report a data breach. However, it needs to be clearly stipulated as to which agency is responsible. Otherwise, the agencies can merely blame each other for any non-reporting.

Within the GIPA Act there is a list of specific parts of which Acts are covered by exemptions regarding secrecy. The Act goes on to state any other secrecy provisions are not sufficient to refuse the release of information. I believe that, in a similar vein,

only certain parts of certain Acts should enable the non-reporting of data breaches. It may be that, even in these cases the Privacy Commissioner should be notified, but the information can be withheld form a general public notice.

As with the GIPA Act, Parliament should determine which provisions of which Acts apply. But, like the GIPA Act the legislation needs to be subject to review and adjustment in the light of experience over time.

As stated in the Discussion Paper, law enforcement agencies are exempt from compliance with certain IPPs. However, a data breach is a different matter. If law enforcement and other agencies don't have to comply with certain privacy requirements, the idea that they also don't face any consequences if they cannot protect the personal information, they hold is a different matter.

The general public have to believe that the personal information they provide to these organisations, if they don't have to comply with certain IPPs, are at least protected from being improperly accessed or released.

We don't want a view that certain government agencies don't care about privacy because they don't have to comply with it.

Should you wish to discuss any of these issues, you should contact me at my home address or by email at [redacted]

Yours sincerely

[redacted]

Senior Consultant

Youngman Consultancy

www.youngmanconsultancy.com.au

[redacted]