New South Wales
Council for Civil Liberties

NSWCCL SUBMISSION

NSW DEPARTMENT OF COMMUNITIES AND JUSTICE

PRIVACY AND PERSONAL INFORMATION PROTECTION AMENDMENT BILL 2021

17 June 2021

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Contact NSW Council for Civil Liberties

http://www.nswccl.org.au
office@nswccl.org.au
Correspondence to: PO Box A1386, Sydney South, NSW 1235

Introduction

1. The NSW Council for Civil Liberties (NSWCCL) welcomes the opportunity to be part of the consultation process and to be invited to make a submission to the NSW Department of Communities and Justice in regard to the draft *Privacy and Information Protection Amendment Bill 2021* (Bill).

2. NSWCCL made a submission to the original 2019 Discussion Paper on 'Mandatory Notification of Data Breaches by NSW Public Sector Agencies' (Discussion Paper). Mandatory data breach notification is a welcome and necessary addition to the NSW public sector privacy regime. It is applicable only to the NSW public sector but has been extended, appropriately, to NSW state owned corporations. Also welcome are the additional regulatory powers, including the power of entry to monitor compliance, granted to the state's Privacy Commissioner.

3. The NSW government has an opportunity to introduce a world standard, effective data breach notification regime. However, the reporting timeframe undermines the objects of the Bill and NSWCCL considers that this renders the Bill seriously flawed.

4. The Factsheet accompanying the Bill explains that the scheme is being proposed because depending on "the size and nature of a data breach, the consequences for individuals can be significant. These consequences can include financial fraud, identity theft and even violence…… Mandatory schemes enable individuals to take action to protect themselves in the event of breaches and can increase public trust in government."[1]

5. Contrary to this purpose, it is possible that an eligible data breach may not be reported to an affected individual or the Privacy Commissioner for at least 30 days.[2] Such a time frame looks to be protecting the interests of public sector agencies at the expense of the individuals whose information is collected and used.

6. The primary purposes of all data breach notification are to:
   - allow consumers to control the use and sharing of their personal information, by ensuring that those affected by a data breach are notified and able to mitigate the damage to them; and
   - compel organisations to improve their data security procedures and policies, by being proactive rather than reactive to a breach.[3] The intention is to increase accountability on the part of public organisations by ensuring that these entities assume responsibility for the information they collect and become accountable for their actions in the storage and use of that data.[4]

7. NSWCCL does not consider that the Bill, as currently drafted, achieves these primary purposes.

---

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

[2] S 59(D)

[3] Smyth, S.M. (2014) Does Australia Really Need Mandatory Data Breach Notification Laws – And If So, What Kind? Journal of Law, Information & Science, Vol. 22, No. 2, 2012-2013 p.3 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2476679

[4] ibid Smyth p.4

Serious harm

8. The Bill provides that a data breach is "eligible" to be reported if it is "likely to cause serious harm to the individual whose information is breached".

9. The European Union General Data Protection Regulation (GDPR) requires individuals to be notified of a data breach where there is a "high risk to the rights and freedom of that person".[5] Both the likelihood and severity of the potential impact is assessed. Sensitive personal data is more likely to be high risk.

   The threshold is high enough to limit notification of any unauthorised breach that may be considered a harmless internal breach unlikely to result in a risk to the rights and freedoms of individuals.

10. The standard of "likely to cause serious harm" is not clearly defined. This is concerning as the relationship between data breaches and the harms suffered as a result, are not straight forward. The Factsheet states that "serious harm can include financial, psychological, physical and reputational harm. What constitutes serious harm will depend on the circumstances of each breach. The legislation will prescribe a number of factors to consider when assessing whether an eligible breach is likely to cause serious harm."[6] The Bill does not prescribe these factors.

    If the eligibility criteria are to be determined on a case-by-case basis, there is incentive to under-report or cover up breaches.

    The Law Society submission to the Discussion Paper recommended a "serious breach" threshold which would capture subjective and objective factors.[7]

11. The NSWCCL preferred position for notification to affected individuals is for eligible breach criteria with a lower threshold than "serious harm" and providing for more objective factors to be taken into account in determining eligibility of a breach.

12. Why does the Bill not require the reporting of most breaches to the Privacy Commissioner or other specially purposed regulatory body? Agencies have a year, from the time the Bill is passed, to put into place systems, policies and procedures to enable effective recognition of data breaches and a swift response.

13. NSWCCL recommends that all data breaches, regardless of their actual or potential to cause harm, should be disclosed to a competent regulatory authority. As a matter of public policy and so as to understand what ongoing or systemic mistakes may be made, the regulatory authority should be aware of all data breaches. Like the GDPR, internal harmless internal breaches could be excluded from the reporting requirement.

---

[5] European Union GDPR 2016/679, Art 34 https://gdpr-info.eu/

[6] Op.cit. Factsheet p.3

[7] Law Society of NSW (2019) Mandatory Notification of Data Breaches by NSW public sector agencies. https://www.lawsociety.com.au/sites/default/files/2020-03/Letter%20to%20Dept%20of%20Communities%20%26%20Justice%20-%20Mandatory%20notification%20of%20data%20breaches%20by%20NSW%20public%20sector%20agencies%20-%2030%20Aug%202019.pdf

Notification time frame.

14. The Bill specifies several time frames in which an agency must assess whether the data breach is an **eligible** breach and then notify the Privacy Commissioner and affected individuals.

15. Several factors have been considered in the Bill in nominating the timeframes, including:

- the need to expeditiously notify individuals so that they can take precautionary action
- the average time in which a malicious breach can lead to misuse of information
- the need to create a workable scheme, including creating timeframes that agencies can comply with, and
- the need to ensure that the Privacy Commissioner has oversight where agencies cannot comply expeditiously with the timeframes (particularly when notifying individuals).[8]

15.1 *In the first instance, a reasonable suspicion of an eligible data breach is formed by an officer or employee of a public sector agency (s59D (1)).*

The section suggests that the officer or employee has formed their own opinion and made a determination as to whether a data breach is **eligible** (Ss 59D (1) & 59E). This is inappropriate as:

15.1.1 If the officer has caused the data breach, they may be deterred from forming this decision.

15.1.2 It is the assessment process that exists to determine whether there has been an eligible breach.

The officer should form a reasonable suspicion of a data breach not of an "eligible" data breach.

15.2 *The officer or employee of a public sector agency, having formed their own suspicion that a data breach is eligible, must report the data breach to the head of the public sector agency.*

NSWCCL considers that officers and employees should report all data breaches to the department head or a superior.

A data breach may signify that the agency has failed to fulfil other obligations in regard to the use and disclosure of personal information. There should be a requirement that every breach involving defined personal information be reported to the Privacy Commissioner, who will then be in a position to take the appropriate action possibly in consultation with the agency, to assess risk to the individual/s.

Reporting all breaches within the criteria also addresses the effects of inadequate or antiquated IT systems and procedures.

[8] Op.cit. Factsheet p.3

15.3 *The head of the agency must immediately make all reasonable efforts to contain the breach, and within 30 days after the reasonable suspicion, expeditiously, assess whether the breach is an eligible data breach.*

30 days is too long a time frame to assess whether a data breach is eligible. If any doubt exists, then for abundant caution, the breach should be considered eligible. The process should not be about avoiding reporting or underreporting. It is about minimising damage to individuals.

A 30-day time frame does not permit individuals, in a timely manner, to take remedial action to protect themselves, such as by cancelling credit cards or changing account passwords. At the least a hacker might sell off data to a third-party for targeted advertising. In the worst-case, a breach might lead to years of financial chaos, harassment or violence against an individual.

The international gold standard practice is set by the mandatory breach notification requirements under the GDPR. Supervisory authorities in the EU must be notified without undue delay, and where feasible, no later than 72 hours after becoming aware of a data breach.[9]

The Privacy Commissioner in the original submission to the Discussion Paper, proposed "a suitable notification time frame in NSW of 10 working days…. having regard to the immediacy of the impact of data breaches that generally require a swift response and remedial action."[10]

The NSWCCL strongly recommends a very short period as a maximum assessment and notification timeframe; certainly, no longer than 10 days.

15.4 *The assessor must advise the head of agency whether a data breach has been found to be an eligible data breach and the head of agency must decide whether an eligible data breach has occurred (s59I).*

NSWCCL considers that the timeframe for the head of agency to form an opinion about whether there is an eligible data breach, must be immediate. Presumably an assessment has been ongoing, and the breach has already been known to the agency head.

15.5 *The public sector agency head must immediately notify the Privacy Commissioner of the eligible data breach (s59L).*

15.6 *The assessment period can be extended by the head of agency (s59J). The Head of agency must however advise the Privacy Commissioner of the extension within 30 days of the reasonable suspicion having been formed of the eligible data breach.*

---

[9] European Union GDPR 2016/679, Art 33 https://gdpr-info.eu/

[10] Information and Privacy Commission (2019) Mandatory Notification of Data Breaches by NSW public Sector Agencies Submission https://www.justice.nsw.gov.au/justicepolicy/Documents/review-mandatory-data-breach-notification/submission-8-information-and-privacy-commission-nsw.pdf

15.7 *As soon as practical after the head of the public sector agency decides an eligible data breach has occurred affected individuals are notified (if reasonably practicable).*

It may be more than 30 days before an affected individual is notified of a data breach. This is unacceptable and undermines the purpose of the Bill. (See 13.3 above)

Notification should be published widely through state media sources rather than only by public notification register which may not be widely seen (s59O).

16. Agencies will need to ensure that systems, policies and procedures are in place to respond swiftly to personal data breaches. The Bill will commence 12 months after it has passed through Parliament. This will enable risk management and employee education by agencies, measures which should increase public confidence in the handling of individuals' information.

Exemptions

17. There are exemptions to mandatory notification to affected individuals. The most concerning are if:

    (a) the head of the agency reasonably believes it would be likely to prejudice an investigation that could lead to the prosecution of an offence or proceeding before a court or tribunal (S59S);
    (b) inconsistent with a secrecy provision(S59U);
    (c) it would worsen the agency's cybersecurity or lead to further data breaches (s59W).

18. In instance (c) above the Privacy Commissioner must be notified of the exemption; the exemption must be reviewed by the agency head each month and provide an update to the Privacy Commissioner; and the exemption lasts only for so long as the agency head deems reasonable considering the nature of the exemption.

    NSWCCL considers that there is no reason why these conditions should not apply to exemptions (a) and (b). Where notification is likely to prejudice an enforcement activity or criminal investigation an argument may be made for that notification to be delayed. In relation to laws that regulate the use or disclosure of information, such as secrecy provisions, oversight bodies much like the Inspector-General of Intelligence and Security (IGIS) and parliamentary joint committees, should be established specifically to oversee operations.[11]

Recommendations

19. The NSWCCL opposes the "likely to cause serious harm" threshold. The NSWCCL preferred position for notification to affected individuals is for eligible breach criteria with a lower threshold than "serious harm" and providing for more objective factors to be taken into account in determining eligibility of a breach.

[11] Op. cit. ALRC

20. NSWCCL recommends that all data breaches, regardless of their actual or potential to cause harm, but other than harmless internal breaches, should be disclosed to a competent regulatory authority.

21. NSWCCL recommends that officers and employees report all data breaches to their department head or a superior.

22. NSWCCL recommends the shortest possible maximum assessment and notification timeframe; certainly, no more than 10 days.

23. NSWCCL recommends that exemptions to mandatory notification of data breach require that the Privacy Commissioner be notified of the exemption; be reviewed by the agency head each month with an update to the Privacy Commissioner; and last only for so long as reasonable considering the nature of the exemption. In some circumstances, notification may be delayed.

24. In all cases there should be independent oversight of the use of the exemption. In relation to laws that regulate the use or disclosure of information, such as secrecy provisions, oversight bodies much like the Inspector-General of Intelligence and Security (IGIS) and parliamentary joint committees, should be established specifically to oversee operations.

25. Countries such as Canada have strong private sector mandatory data breach reporting regimes.[12] NSWCCL recommends that NSW introduces similar legislation dealing with private sector data breaches, as a matter of urgency.

This submission was prepared by [redacted] on behalf of the New South Wales Council for Civil Liberties.

Yours sincerely

[redacted]

[redacted]

Contact in relation to this submission- [redacted]
email [redacted]
tel [redacted]

[12] *Personal Information Protection and Electronic Documents Act* (PIPEDA) https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/