New South Wales
Council for Civil Liberties

NSWCCL SUBMISSION

NSW DEPARTMENT OF COMMUNITIES AND JUSTICE

MANDATORY NOTIFICATION OF DATA BREACHES BY NSW PUBLIC SECTOR AGENCIES

DISCUSSION PAPER

19 August 2019

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
Street address: Suite 203, 105 Pitt St, Sydney, NSW 2000, Australia
Correspondence to: PO Box A1386, Sydney South, NSW 1235
Phone: 02 8090 2952
Fax: 02 8580 4633

MANDATORY NOTIFICATION OF DATA BREACHES BY NSW PUBLIC SECTOR AGENCIES

Introduction

The New South Wales Council of Civil Liberties (NSWCCL) welcomes the opportunity to make submissions to the New South Wales Department of Communities and Justice. The Discussion Paper asks for feedback in relation to the mandatory notification of data breaches by NSW public sector agencies.

NSWCCL supports the introduction of a mandatory notification of data breaches by NSW public sector agencies. Further, NSWCCL supports wider mandatory notification of privacy breaches by New South Wales public sector agencies.

Specific responses to the Discussion Paper questions are set out in this submission.

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

NSWCCL supports the introduction of a mandatory data breach notification scheme for NSW public sector agencies.

As set out in the Discussion Paper, the reasons to have such a scheme, include:

- The NSW government has a high level of responsibility for collection, use and storage of personal information.
- Where data breach occurs there may be a real risk of serious harm to the affected individual. Informing individuals of privacy breaches, in a timely manner, allows them to take remedial action to protect themselves and avoid adverse consequences
- If agencies report data breaches it demonstrates their ability to manage data breaches; strengthens data breach and privacy processes; reinforces accountability; and maintains trust with the public
- It is considered best practice, in many jurisdictions, to introduce a mandatory data breach notification scheme.
- The Australian community expects to be told when a data breach occurs.
- Reducing under-reporting of breaches.
- Having a consistent approach and standardisation of security systems.

NSWCCL adds that:

i) Commonwealth legislation dealing with notifiable data breaches is undermined without NSW and other States legislation, to support it.

ii) The risk to the privacy and financial security of individuals, as a result of widespread collection of personal information, is growing. Agencies need incentives to change the way they handle and store consumer information in order to reduce the risk that the security of information will be breached.[1] Mandatory data breach notification provides a strong incentive for the enhancement of information security measures.[2]

iii) Reducing security breaches is a legitimate and important policy goal, reinforcing that personal and sensitive information will be handled responsibly.[3]

iv) Agencies will be encouraged to be more transparent about their information handling processes.

Recommendation 1

NSWCCL strongly recommends that the NSW government introduce a mandatory data breach notification scheme for NSW public sector agencies.

Question 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 Principal has occurred?

(a) Unauthorised access or disclosure occurs due to malicious action, human error or a failure in information handling security. Reporting is therefore an important step in ensuring government accountability and creates trust in agency systems.

Unauthorised access to or disclosure of personal information by one NSW public sector agency from another public sector agency must also be reported. Each public sector agency enters into a separate custodial obligation, with relevant NSW citizens, of their private information. Interagency breach could have severe consequences, for example, in relation to the compromise of identity information in domestic abuse matters.

The decision to notify may be made in consultation with the Privacy Commissioner. Where the threshold for notification is definitely not met such consultation would not be required. For example, where information is disclosed by accident or in good faith but not used further in unauthorised disclosure, the information is already in the public domain or there is temporary loss.

Notifying the Privacy Commissioner also provides an opportunity to monitor for continuous systemic breaches.

[1] Winn, J.K. (2009) Are "better" security breach notification laws possible? *Berkeley Technology Law Journal* Vol. 24 No.3 pp 1133-1165 at 1133
[2] Bisogni, F. (2016) Proving limits of state data breach notification laws: is a federal law the most adequate solution? *Journal of Information Policy* vol 6 pp 154-205 at 190
[3] Winn op cit 1142 & 1160

(b) If a significant reduction in data breaches is a serious policy goal then, not just access and disclosure breaches, but general information security needs to be addressed.[4] Privacy risks are amplified with the increasing use of automated decision making in public sector agencies. Information can be collected and used in a way that disadvantages or discriminates against a person, or group, without them being aware of it. Automated decision making can lead to profiling and, importantly, avenues for making complaints are rendered redundant in these situations.

Reporting breaches that also relate to the collection, use and storage of information assists in the continuous assessment of privacy and disclosure risks.

Recommendation 2

NSWCCL supports the enactment of legislation requiring NSW public sector agencies to report breaches where both unauthorised access to or disclosure of personal information occurs.

Recommendation 3

NSWCCL recommends that legislation include the requirement that NSW public sector agencies report interagency breaches of unauthorised access to or disclosure of personal information.

Recommendation 4

NSWCCL supports the enactment of legislation requiring NSW public sector agencies to report breaches where any breach of an IPP has occurred.

Question 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 describe the factors an agency must consider when assessing whether a data breach meets the threshold of serious harm?

(a) The European Union General Data Protection Regulation (*GDPR*), that requires individuals to be notified of a data breach where there is a "high risk to the rights and freedom of that person", is a desirable standard to apply.[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.

[4] Winn op cit 1137
[5] European Union GDPR 2016/679, Art 34

(b) If the standard "a real risk of serious harm" is adopted then it needs to be clearly defined. The relationship between data breaches and the harms suffered as a result are not straight forward. International law defines the standard as "a reasonable degree of likelihood" and "a real and substantial risk".[6]

(c) Factors an agency must consider when assessing a data breach should be prescribed. Without guidance an objective assessment of serious harm, is difficult.

Some factors are set out in point 4.9 of the Discussion Paper. Other factors to consider when assessing if a data breach is likely to cause serious harm or if there is a high risk to the rights of that person, are:

i) The cause and extent of the breach, i.e is it ongoing?;

ii) Who is affected and the severity of the consequences for them;

iii) The volume of personal data breached;

iv) The ease of identification of affected individuals.

Recommendation 5

NSWCCL recommend the adoption of the GDPR standard, "high risk to the rights and freedom of that person", for determining the threshold for notification of an information breach.

Recommendation 6

NSWCCL recommends that if the standard "a real risk of serious harm" is adopted then it needs to be clearly defined.

Recommendation 7

NSWCCL recommends that legislation should describe the factors an agency must consider when assessing whether a data breach meets the threshold of serious harm, including, but not limited to, the extent of the breach, the volume of information breached and the ease of identification of the individual affected.

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?

[6] Australian Law Reform Commission, 51. Data Breach Notification *Australian Privacy Law and Practice (ALRC Report 108), see R v Secretary of State for the Home Department, Ex parte Sivakumaran [1988] AC 958. <https://www.alrc.gov.au/publications/51.%20Data%20Breach%20Notification/alrc%E2%80%99s-view#_ftn133>*

A data breach may signify that the agency has failed to fulfil other obligations in regard to the use and disclosure of personal information. As with the proposed model recommended for Canada, "there should be a requirement that every breach involving defined personal information be reported to the Privacy Commissioner, with full information about the nature and extent, the anticipated risks, mitigation measures, steps taken to notify affected individuals or, where notification is not considered warranted, the justification for not taking this step."[7] The Privacy Commissioner 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 in place. Reporting breaches only when remedial action has been unsuccessful, encourages a policy of mitigation of damage, after the fact, instead of reducing the risk that the problem will occur in the first place.

Recommendation 8

NSWCCL recommends that NSW public sector agencies should report data and any of the breach involving defined personal information, whether remedial action has prevented serious harm, or not.

Question 5
(a) what information should be notified to the NSW Privacy Commissioner and affected individual in relation to data breaches?
(b) should the legislation prescribe the form and content of the notification?

(a) See responses to Question 4. In identifying what information should be notified to the Privacy Commissioner and the affected individual, consideration should be given to managing the level of communication to the individual not safeguarding the circumstances of the breach. Underreporting should be avoided.[8]

In California, the event that triggers the obligation to provide notice is any 'breach of the security of the system', though as previously described there are exceptions to the general obligation to notify for 'harmless internal breaches'.[9]

The information in a notification scheme should include that which is in the Information and Privacy Commissioner (*IPC)* voluntary notification scheme. Further to this list can be added:

i) Details of the number affected

ii) A clear recommendation to the individual to reduce breach related risks.

iii) Fostering interaction with affected individuals by making support available to them.

[7] ALRC op cit
[8] Bisogni op cit 192
[9] ALRC op cit

iv) The timing of breach detection and notification dates so that the individual is aware of their uninformed exposure.[10]

v) Measures taken to prevent a re-occurrence of the breach.[11]

(b) As individuals must rely on the notification to understand the seriousness of the situation and be adequately alerted, the form should be mandatory or have mandatory elements. A mandatory prescriptive and standardised template may also be a useful reference for agencies.

Recommendation 9

NSWCCL recommends that the NSW Privacy Commissioner and affected individuals be notified with information as set out in the IPC voluntary notification scheme, as well as details of the numbers of those affected, recommendations to reduce risk, available support for those affected, the timing of uninformed exposure and measures to prevent a re-occurrence of the breach.

Recommendation 10

NSWCCL recommends that legislation prescribe the form and content of the notification.

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

NSWCCL considers the European Union position to be best practice. Data breaches should be reported to the relevant regulator "without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach."[12] Rapid notice to the individual, that a breach has occurred, helps them to minimise the damage that occurs from that breach.

In California, and most other US states with data breach notification laws, notification must occur in "the most expedient manner possible and without unreasonable delay."[13] Circumstances where notification may be permitted over 72 hours, might include similar breaches occurring over a short period or where a complex investigation is required. In the latter case an initial incomplete notification might be made.[14]

Recommendation 11

[10] Bisogni op cit 190
[11] ALRC op cit
[12] European Union General Data Protection Regulation 2016/679, Article 33
[13] ALRC op cit
[14] Pearson, C. & Zhu, X. (2018) Notification of data breaches under the GDPR-10 Frequently Asked Questions *Cleary Cybersecurity and Privacy Watch* < https://www.clearycyberwatch.com/2018/01/notification-data-breaches-gdpr-10-frequently-asked-questions/>

NSWCCL recommends that legislation prescribe that information breaches be reported without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach.

Question 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?

(a) The NSW Privacy Commissioner requires additional power to ensure compliance with a mandatory notification scheme particularly given that the NSWCCL supports reporting of all privacy breaches, not just unauthorised information disclosures. Complaints systems are insufficient if an individual is not aware that their information has been compromised, therefore the Privacy Commissioner should have the ability to investigate all breaches without a complaint having been made.

The NSW Privacy Commissioner should be able to mandate that agencies develop a written program that identifies and detects the relevant warning signs of unauthorised disclosure. This could prescribe appropriate responses that would prevent and mitigate the risk and detail a plan to update management systems.

(b) Emphasis on collaboration and selective punitive enforcement in response to wilful non-compliance, is most likely to achieve compliance.[15] Civil penalties are also useful where there have been serious or repeated interference with an individual's privacy.

Recommendation 12

NSWCCL recommends that the NSW Privacy Commissioner be endowed with additional powers to encourage compliance with a mandatory notification scheme, including requiring the reporting of all information breaches not just those relating to disclosure, wider investigative powers and mandatory management and systems programs.

Recommendation 13

NSWCCL recommends that monetary penalties apply to public sector agencies and civil remedies be made available, where repeated or wilful noncompliance occurs.

Question 8
What exemptions from the requirement to notify individuals and the New South Wales Privacy Commissioner of eligible data breaches, should apply?

[15] Winn op cit 1159

Too many or inconsistent exceptions in reporting data breaches, can lead to under-reporting.

There should be no exemption where information is held jointly with another entity. All entities should be notified. 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.[16]

Recommendation 14

NSWCCL does not recommend exemptions from the requirement to notify individuals or the Privacy Commissioner, of eligible data breaches unless, in the case of security agencies, there is other independent oversight of the relevant agency or where there is good reason to delay notification, such as likely prejudice to a criminal investigation.

This submission was prepared by Michelle Falstein, Convenor of NSWCCL Privacy Action Group, on behalf of the New South Wales Council for Civil Liberties. We hope it is of assistance to the New South Wales Department of Communities and Justice.

Yours sincerely,

Therese Cochrane
Secretary
NSW Council for Civil Liberties
[redacted]

[redacted]

[16] ALRC op cit