THE LAW SOCIETY OF NEW SOUTH WALES
YOUNG LAWYERS

Submission in response to the *Privacy and Personal Information Protection Amendment Bill 2021*

16 July 2021

Policy Reform & Legislation,
Department of Communities and Justice,
GPO Box 31,
Sydney NSW 2001

By email: policy@justice.nsw.gov.au

Contact: [redacted]

Contributors: [redacted]

Managing Editor: [redacted]

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

The NSW Young Lawyers Communications, Entertainment and Technology Law Committee makes the following submission in response to the *Privacy and Personal Information Protection Amendment Bill 2021*.

NSW Young Lawyers

NSW Young Lawyers is a division of The Law Society of New South Wales. NSW Young Lawyers supports practitioners in their professional and career development in numerous ways, including by encouraging active participation in its 15 separate committees, each dedicated to particular areas of practice. Membership is automatic for all NSW lawyers (solicitors and barristers) under 36 years and/or in their first five years of practice, as well as law students. NSW Young Lawyers currently has over 15,000 members.

The NSW Young Lawyers Communications, Entertainment and Technology Law Committee (**Committee**) aims to serve the interests of lawyers, law students and other members of the community concerned with areas of law relating to information and communication technology (including technology affecting legal practice), intellectual property, advertising and consumer protection, confidential information and privacy, entertainment, and the media. As innovation inevitably challenges custom, the Committee promotes forward thinking, particularly with respect to the shape of the law and the legal profession.

Summary of Recommendations

The Committee welcomes the opportunity to comment on the *Privacy and Personal Information Protection Amendment Bill 2021* (**the Bill**) and, in particular, the mandatory notification of data breach (**MNDB**) scheme on behalf of NSW Young Lawyers. The Committee has the following recommendations:

1. The Committee submits that if the Bill is enacted, it will strengthen privacy protections for individuals. The implementation of a MNDB scheme at the state level will fulfil a key gap in privacy regulation, by ensuring that NSW public sector agencies are subject to the same obligations as their Commonwealth counterparts. The Committee therefore supports the introduction of a MNDB scheme for NSW public sector agencies and applicable state-owned corporations (**SOCs**).

2. The Committee supports the proposed changes to the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**) that will extend its provisions to include SOCs.

3. The Committee recommends that contracted service providers be defined in the PPIP Act and expressly included within the scope of the MNDB Scheme.

4. The Committee recommends that "serious harm" be defined by reference to readily identifiable outcomes of data disclosure.

5. The Committee submits that the Privacy Commissioner should be allowed a power to award compensation at the complaint stage to encourage cost effective procedures and efficiency.

6. The Committee submits that the monetary limit should be removed to provide complainants with full compensation for the loss actually suffered.

7. The Committee submits that in addition to notification requirements set out in section 59L of the Bill, there should be a requirement that agencies to put in place proactive cybersecurity measures and meet industry standards for data management as a means of prevention.[1]

8. The Committee submits that agencies should be held accountable for the data breaches if negligible use of data is found during the investigation process.

[1] Ross Schulman, 'Disincentives to Data Breach: Problems with Notification and Future Legislative Possibilities' (2009) 1(2) Legislation and Policy Roundtable [xxiii].

Part A: MNDB Scheme – Strengths

Introduction

1. The Committee submits that if the Bill is enacted, it will strengthen privacy protections by providing greater certainty, empowering individuals, improving data management, reducing the occurrence of data breaches, increasing an agency's capability to respond to data breaches, and reducing underreporting. As a result, this will increase public trust in agencies.

Providing Certainty

2. The Committee submits that if the Bill is enacted, it will 'provide certainty for the public and government agencies regarding rights and obligations around the handling of personal information'.[2]

3. The Commonwealth notification data breach (**NDB**) scheme currently in place is aimed primarily at private sector organisations and federal government agencies that are regulated by the *Privacy Act 1988* (Cth) (**Privacy Act**). The NSW MNDB scheme will provide greater certainty, as it proposes to fill this gap by expanding the same notification threshold to public sector entities regulated by the Privacy Act and to NSW SOCs that are not already regulated by it. The Bill also proposes to repeal section 117C of the *Fines Act 1996* (NSW) to ensure that all NSW public sector agencies are regulated by the same mandatory notification scheme.

4. A legislated mandatory notification scheme will provide greater certainty for both the public and government agencies about what entities are required to provide data breach notifications, what data breaches should be reported, who should be notified, and how they should be notified, by explicitly setting out their respective rights and obligations and the actions that should be taken if a data breach occurs.

5. Furthermore, the MNDB scheme will apply the many features of the Privacy Act that apply for data breaches. This helps provide further certainty in cases where a breach may be notifiable under both the NDB and MNDB schemes, as agencies will be able to follow similar processes and procedures to comply with both schemes.

---

[2] Department of Communities and Justice, Parliament of New South Wales, *Privacy and Personal Information Protection Amendment Bill 2021: Factsheet* (Factsheet, 2021) 2.

Empowering Individuals

6. The Bill, if enacted, will also 'enable individuals to take action to protect themselves in the event of breaches and provide individuals with information needed to reduce their risk of harm following a serious data breach'.[3]

7. The DCJ's proposed MNDB scheme sets out the information that should be communicated to individuals if their personal information is the subject of a data breach. This includes details regarding the eligible data breach, affected data and the affected agency, as well as recommendations about the steps the individual should take in response to the breach. The Committee considers that timely notification to both individuals and the NSW Privacy Commissioner will enable individuals to take proactive steps to mitigate the risks, avoid adverse consequences and protect themselves.[4]

8. Furthermore, if a data breach were to also invoke obligations under the NDB scheme, individuals are additionally empowered as they will have reassurance that a data breach involving their personal information imposes the same obligations upon an agency, irrespective of whether it is at the State or Commonwealth level.

Improving Data Management, Reducing the Occurrence of Breaches & Increasing Response Capability

9. The Committee furthermore submits that the Bill, if enacted, will encourage agencies to consider their data management processes.

10. The MNDB scheme will require agencies to satisfy certain data management requirements, such as having a publicly accessible data breach policy and maintaining an internal data breach incident register.

11. Agencies require an incentive to consider the inefficiencies in their risk and data management processes, and to change the way they handle and store personal information.[5] The MNDB scheme will improve transparency and accountability of agencies in the way they respond to data breaches and will make them

---

[3] Ibid.
[4] NSW Council for Civil Liberties, Submission No 7 to the Department of Communities and Justice, *Mandatory Notification of Data Breaches by NSW Public Sector Agencies Discussion Paper* (19 August 2019) 1; Mamoun Alazab, Seung-Hun Hong and Jenny Ng 'Louder Bark with No Bite: Privacy Protection through the Regulation of Mandatory Data Breach Notification in Australia' (2021) 116 *Future Generation Computer Systems* 1, 26.
[5] NSW Council for Civil Liberties, Submission No 7 to the Department of Communities and Justice, *Mandatory Notification of Data Breaches by NSW Public Sector Agencies Discussion Paper* (19 August 2019) 2; Flora J Garcia, 'Data Protection, Breach Notification, and the Interplay between State and Federal Law: The Experiments Need More Time' (2007) 17 *Fordham Intellectual Property, Media and Entertainment Law Journal* 693, 701.

more aware of the importance of risk and data management. It will also encourage agencies to actively take steps to prevent serious harm to individuals from data breaches, such as by putting substantial privacy and cybersecurity controls in place to increase their capability to properly respond to, mitigate and manage future data breaches.[6]

Reducing Underreporting

12. The Committee is concerned that data breaches may be underreported under the current voluntary data breach reporting scheme.

13. The Committee notes that in the year before the NDB scheme was introduced, the Office of the Australian Information Commissioner (**OAIC**) received 159 data breach notifications. However, during the first year of the NDB scheme's implementation, the OAIC received 1,132 notifications, representing a 712% increase in data breach notifications within 12 months.[7]

14. If such results from the Commonwealth NDB scheme are indicative of reporting trends, the MNDB scheme could also reduce the tendency for data breaches to go unreported, especially in circumstances where state agencies and SOCs may have previously not reported notifiable data breaches as a result of not being covered by the NDB scheme.

Increasing Public Trust

15. The Committee submits that the Bill, if enacted, will also 'increase public trust in government and agency handling of personal information and data breach incidents'.[8]

16. The Deloitte Australian Privacy Index 2019 found that there has been a significant drop in the trust in government when it comes to privacy in recent years. The government was ranked number three in 2018 and then dropped to number eight in 2019.[9] The OAIC Australian Community Attitudes to Privacy Survey 2020 also found that only 45-56% of Australians consider the government trustworthy with regards to the

---

[6] Jane K Winn, 'Are "Better" Security Breach Notification Laws Possible?' (2009) 24(3) *Berkeley Technology Law Journal* 1133, 1133; Fabio Bisogni, 'Proving Limits of State Data Breach Notification Laws: Is a Federal Law the Most Adequate Solution?' (2016) 6 *Penn State University Press* 154, 190; Mark Burdon, Bill Lane and Paul von Nessen, 'The Mandatory Notification of Data Breaches: Issues arising for Australian and EU Legal Developments' (2010) 26(2) *Computer Law & Security Review* 115.
[7] Office of the Australian Information Commissioner, *Notifiable Data Breaches Scheme 12-Month Insights Report* (Insights Report, 13 May 2019) 4.
[8] Department of Communities and Justice (n 1) 2.
[9] Deloitte, 'Deloitte Australian Privacy Index 2019' (Web Page, 2019) 8 <https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-privacy-index-150519.pdf>.

collection and use of their biometric information,[10] and 83% of Australians would like the government to do more to protect the privacy of their data.[11]

17. Ultimately, data breaches can lead to a loss of confidence and trust in agencies that handle personal information. As discussed above, the Committee considers that the MNDB scheme will improve transparency and accountability of agencies in the way they respond to data breaches. It will also encourage agencies to improve their practices and policies to better prevent, mitigate and manage the risk of data breaches.[12] This protection of people's privacy is fundamental to public trust and confidence.

18. The Committee also notes that, but for iCare's submission, all publicly accessible submissions to the Department of Communities and Justice's 'Mandatory Notification of Data Breaches by NSW Public Sector Agencies Discussion Paper' support the introduction of a MNDB scheme. These submissions were received from a wide range of stakeholders including government agencies, councils, educational facilities and advocacy groups. Accordingly, the introduction of the MNDB scheme will arguably be in line with the wider community and public interests and expectations.

Conclusion

19. The implementation of a MNDB scheme at the state level will fulfil a key gap in privacy regulation.[13] The Committee supports the introduction of a MNDB scheme for NSW public sector agencies and SOCs.

---

[10] Office of the Australian Information Commission, Parliament of Australia, *Australian Community Attitudes to Privacy Survey 2020* (Survey, September 2020) 83.
[11] Ibid 65.
[12] Jane K Winn, 'Are "Better" Security Breach Notification Laws Possible?' (2009) 24(3) *Berkeley Technology Law Journal* 1133, 1133; Fabio Bisogni, 'Proving Limits of State Data Breach Notification Laws: Is a Federal Law the Most Adequate Solution?' (2016) 6 *Penn State University Press* 154, 190; Mark Burdon, Bill Lane and Paul von Nessen, 'The Mandatory Notification of Data Breaches: Issues arising for Australian and EU Legal Developments' (2010) 26(2) *Computer Law & Security Review* 115.
[13] Deloitte Risk Advisory Pty Ltd, Submission No 12 to the Department of Communities and Justice, *Mandatory Notification of Data Breaches by NSW Public Sector Agencies Discussion Paper* (23 August 2019) 2.

Part B: The Extension of the PPIP Act to SOCs

Introduction

20. In its present form, the PPIP Act does not apply to NSW SOCs. The proposed amendments in the Bill would extend the provisions of the PPIP Act to all SOCs, except Essential Energy, which is regulated under the Privacy Act.

Expansion of Definition

21. By expanding the definition of 'public sector agency' in the PPIP Act to include 'a state-owned corporation that is not subject to the Privacy Act of the Commonwealth,' the following SOCs will have to adhere to the provisions of the PPIP Act:[14]
    (i) Transport Asset Holding Entity of NSW;
    (ii) Forestry Corporation of NSW;
    (iii) Hunter Water;
    (iv) Port Authority of NSW;
    (v) Sydney Water;
    (vi) Landcom, and
    (vii) Water NSW.

22. These SOCs are currently not subject to NSW privacy laws, though some have voluntarily elected to follow the PPIP Act.[15] This has led to a lack of accountability and consistency in the way privacy information has been handled by SOCs. There have also been increasing concerns amongst Australians about the protection of their privacy and the impact new technological developments have on their personal information.

23. A privacy survey conducted by the Australian Information Commissioner in 2020 found that 40% of those surveyed felt their personal information was poorly protected and that 83% of Australians would like the government to do more to protect their data privacy.[16] NSW SOCs have access to a significant amount of personal information about the people of NSW.[17] For example, Sydney Water possesses confidential files and medical records, as well as customers' personal information.[18] If other state agencies are subject to the PPIP Act for possessing sensitive information about their consumers, then it is clear that SOCs should be as well.[19]

---

[14] Privacy and Personal Information Protection Amendment Bill 2021 (NSW) sch 1 item 2.
[15] Information and Privacy Commission NSW, *State Owned Corporations (SOCs) and Your Right to Government and Personal Information* (Fact Sheet, September 2020) <https://www.ipc.nsw.gov.au/fact-sheet-state-owned-corporations-socs-and-your-right-government-and-personal-information>.
[16] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020* (Survey, September 2020) 64-65.
[17] NSW, *Parliamentary Debates,* Legislative Assembly, 14 November 2019, 1585 (Paul Lynch).
[18] Sydney Water, *Agency Information and Guide 2020* (May 2020) 12.
[19] NSW, *Parliamentary Debates,* Legislative Assembly, 14 November 2019, 1585 (Paul Lynch).

Opt-in option

24. Section 6F of the Privacy Act provides that a SOC may opt into the Commonwealth privacy regime.[20] However, this opt-in model does not guarantee total compliance, as SOCs can simply chose to not be bound by the Privacy Act and the Australian Privacy Principles (**APP**). The 2015 Report of the Privacy Commissioner indicates that only three out of the ten NSW SOCs at the time had elected to follow the Commonwealth regime and as a result, only specific consumers had any formal privacy protection.[21]

25. With some SOCs opting to comply with the federal Privacy Act and the APP, and others choosing to be bound by the PPIP Act and the 12 Information Protection Principles, there are major inconsistencies and gaps in the way privacy and personal information is being handled by NSW SOCs.[22] For example, the PPIP Act does not contain a model that allows for the external review of complaint handling, whereas the Commonwealth regime sets out various options for handling complaints.[23] The expansion of the PPIP Act to include SOCs would result in consumers finally having a consistent level of privacy protection.

26. SOCs were initially excluded from the PPIP Act as the NSW Government wanted to ensure parity between private commercial businesses and SOCs in terms of their privacy obligations.[24] However, since then SOCs have been legislatively integrated into the government sector and this initial rationale is no longer relevant.[25] If private sector businesses must comply with the Privacy Act when they meet a certain size threshold, it is reasonable that SOCs are regulated under a similar consistent framework under the Privacy Act, where the SOC meets that same annual turnover threshold.[26]

Conclusion

27. Should the Bill pass, this would result in greater consistency in the way an individual's personal information is handled by SOCs, leading to stronger privacy protections for consumers and the people of NSW.

---

[20] NSW Privacy Commissioner, *Report of the Privacy Commissioner under Section 61B of the Privacy and Personal Information Protection Act 1988* (Report, February 2015) 19.
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] Ibid.

Part C: MNDB Scheme – Potential Challenges

Extension of Responsibility

28. Firstly, the Committee submits that there is ambiguity in the Bill's extension of responsibility, specifically in relation to contracted service providers. The Bill contains no provision that expressly includes contracted private organisations in the MNDB scheme.

29. It is noted that this extension of responsibility is intentionally absent from the Privacy Act. As it stands, contracted service providers in relation to state contracts, particularly managed service providers (**MSPs**), are exempt from the Commonwealth MNDB Scheme.[27] Logically, MSPs providing services under a state contract should be captured by the state legislation. However, this is not the case as the PPIP Act only extends its privacy obligations to persons or bodies that provide data services.[28]

30. It is noted that the *Privacy and Personal Information Protection Amendment (Service Providers) Bill 2020* (NSW) was introduced to the Legislative Assembly with a view to capturing MSPs in state privacy obligations under the PPIP Act. It was noted that the exclusion of MSPs left a 'wide field uncovered',[29] considering the prevalence of government outsourcing to MSPs. The Committee notes that the Bill did not pass through the Legislative Council in September 2020.

31. Accordingly, any contracted service provider who provides a service other than data collecting, processing, or disclosure services could arguably sit in the penumbra between both the Commonwealth and State legislation when it comes to active regulation. It is also worth noting that MSPs featured prominently in the most recent Notifiable Data Breach report published by the OAIC.[30]

32. It is recommended that contracted service providers be defined in the PPIP Act and expressly included within the scope of the MNDB Scheme.

---

[27] *Privacy Act 1988* (Cth) s 7B(5).
[28] *Privacy and Personal Information Protection Act 1998* (NSW) s 3(g)(i).
[29] Second Reading Speech, *Privacy and Personal Information Protection Amendment (Service Providers) Bill 2020,* https://www.parliament.nsw.gov.au/Hansard/Pages/HansardResult.aspx#/docid/'HANSARD-1323879322-111128'
[30] OAIC, Notifiable Data Breaches Report: July-December 2020 <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2020/>.

Definition of Serious Harm

33. Secondly, the Committee submits that a definition of 'serious harm' be included in the Bill. Under the proposed section 59C, an eligible data breach will have occurred where personal information has been lost, the disclosure of which a reasonable person would likely to conclude would result in serious harm to the individual to whom the information relates.

34. Under the Privacy Act, section 26WG provides factors that may assist in determining whether disclosure of information would be likely to result in serious harm. Those factors largely align with those proposed under section 59G of the Bill.

35. Notwithstanding this guidance, there is still ambiguity in relation to the 'other relevant matters' that may be considered.

36. The Committee submits that resolving this ambiguity is relevant given that the time it takes for an organisation to assess a breach and determine whether harm is serious potentially increases the risk of the inefficacy of such assessments, particularly where the relevant entity is under resourced.

37. To provide further clarity, the Committee recommends that the nature of the harm that has occurred or may occur be further clarified, for example:
    (i) financial loss;
    (ii) damage to reputation;
    (iii) psychological distress;
    (iv) the disclosure of sufficient identifying information to permit identity fraud;
    (v) enabling unauthorised access to information or services in the name of the individual by a person other than the individual; and

Compensation

38. Finally, it is submitted that the Bill does not adequately address the shortcomings of the PPIP Act in relation to compensation for individuals affected by an eligible data breach. Although the PPIP Act provides for the making of a complaint to the Privacy Commissioner,[31] and resolution of such a

[31] *Privacy and Personal Information Protection Act 1998* s 45.

complaint by way of conciliation,[32] the Privacy Commissioner is not empowered to make an award of damages or compensation to resolve a complaint.[33]

39. The only mechanisms by which compensation may be provided to a complainant are through the internal review process conducted by the agency itself,[34] or following administrative review by the NSW Civil and Administrative Tribunal (**NCAT**).[35] This is distinct from the federal OAIC's powers to declare that the complainant is entitled to compensation under the Commonwealth Privacy Act.[36] It is submitted that allowing for compensation to be recommended by the NSW Privacy Commissioner at the complaint stage would be more cost effective and efficient for complainants than requiring the matter to progress to the NCAT before compensation can be awarded.

40. It is also submitted that the limitation of compensation awarded under the PPIP Act to $40,000 is unnecessary. Although the average cost of identity theft resulting from data breaches is only $300, the Australian Institute of Criminology has recorded individual losses of up to $1,000,000.[37] Depending on the seriousness of the harm inflicted, the existing limitation of the compensation that may be awarded under the PPIP Act could preclude fair compensation for losses incurred as a result of identity theft. It is also worth noting that statutory limits to compensation have been criticised by the High Court of Australia as resulting in injustice where full compensation cannot be awarded.[38]

41. Accordingly, it is submitted that the monetary limit should be removed to provide complainants with compensation for loss actually suffered.

---

[32] Ibid s 49.
[33] Information and Privacy Commission New South Wales, 'Fact Sheet – IPC Privacy Statement of Jurisdiction' *Information and Privacy Commission* (Web Page, May 2019) < https://www.ipc.nsw.gov.au/fact-sheet-ipc-privacy-statement-jurisdiction>.
[34] *Privacy and Personal Information Protection Act 1998* s 53.
[35] Ibid s 55.
[36] *Privacy Act 1998* (Cth) s 52(1)(b)(iii).
[37] Australian Institute of Criminology, 'Counting the costs of identity crime and misuse in Australia, 2018-19' (AIC Reports No 28) p 7 < https://www.aic.gov.au/sites/default/files/2020-08/sr28_counting_the_costs_of_identity_crime_and_misuse_australia_2018-19.pdf>.
[38] *Australian Iron & Steel Pty Ltd v Banovic* (1989) 89 ALR 1, 32.

Part D: MNDB Scheme: Other points of interest

Proactive Measures

42. As part of an agency's privacy obligations under the PPIP Act, personal information that agencies collect must be stored securely and be protected from unauthorised access.[39] While the Bill addresses the point at which a breach of personal information has occurred, more emphasis should be placed on proactive measures such as ensuring that agencies have adhered to the NSW Government's Cyber Security Policy which specifies 25 mandatory cyber security requirements that agencies must implement.[40]

43. In an interview with Chief Information Security Officers from the Health Care sector in the United States, it was communicated that breach notification laws in the United States have led to an increase of resources allocated to encryption mechanisms, and affected the budget and resources previously allocated to other critical areas of information security.[41] This view strengthens the approach that having comprehensive cybersecurity regulations, in addition to data breach notification regulation, is more effective in the prevention of data breaches than a standalone requirement to notify when a breach occurs.[42]

44. Article 35 of the European General Data Protection Regulation (**GDPR**) sets out a requirement to carry out a Data Protection Impact Assessment (**DPIA**) which is a process that identifies and minimizes data protection risks.[43] Article 35 of the GDPR sets out the main requirements of the DPIA's contents as follows:[44]

    (i) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

    (ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

    (iii) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph (i); and

---

[39] *Privacy and Personal Information Protection Act 1998* (NSW) s 12.
[40] NSW Government, *NSW Cyber Security Policy* (Policy, 2021) <https://www.digital.nsw.gov.au/sites/default/files/NSW%20Cyber%20Security%20Policy%202021%204.0.pdf>.
[41] David Thaw, 'Data Breach (Regulatory) Effects' [2015] 2015 Cardozo Law Review De-Novo 151.
[42] Ibid.
[43] General Data Protection Regulation [2016] OJ L 119/679, art 35.
[44] Ibid.

(iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data, and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

45. The DPIA was designed to help organisations with risk assessments related to data processing practices that may result in a data breach and harm to the individual.[45] The DPIA is based on a proactive approach to data security which allows for an early intervention, giving the agency the opportunity to increase privacy protections and mitigate potential harm.

46. Australian state and federal regulators should have an incentive to adopt a proactive approach in order to improve consumer trust in the security of their information at the hands of public sector agencies.

Unintended Use

47. Often, we see companies collecting data from customers for purposes other than carrying out the intended transaction.[46] These often come in the form of cluttered 'promotions' or 'spam' email inboxes, where the same companies' consumers have engaged with for a single transaction, continue to send communications until such time as the consumer chooses to 'unsubscribe'.

48. The APP provide that 'an agency may only solicit and collect personal information that is reasonably necessary'.[47] This requirement places a responsibility on the agencies that collect, use and handle personal information to ensure that only the necessary information for the purposes of the transaction is collected. An example of when the collection of unnecessary information can cause a breach is when an agency sends out an Electronic Direct Mail (**EDM**) to their entire mailing list and forgets to blind carbon copy (bcc) the recipients. This results in the email addresses of the recipients being exposed and available for access to anyone on that mailing list. This incident could amount to a 'notifiable data breach' as email addresses often contain an individual's name.

49. When investigating and monitoring agencies who have reported a data breach under section 59Y of the Bill, the Privacy Commissioner should consider whether agencies policies and practices were

---

[45] Annie Greenley-Giudici, 'EU GDPR Article 35 – Data Protection Impact Assessment (DPIA), Part I', *TrustArc* (Online, Oct 10, 2017) <https://trustarc.com/blog/2017/10/10/eu-gdpr-article-35-data-protection-impact-assessment-dpia-part/>.
[46] Business News Daily, 'How Businesses Are Collecting Data (And What They're Doing With It)' (Web Page, 2020) <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>.
[47] Office of the Australian Information Commissioner, *Chapter 3: APP 3 – Collection of solicited personal information* (Australian Privacy Principles guidelines, 22 July 2019).

insufficient when handling the personal information or allowed for the collection of unnecessary information. If the Privacy Commissioner subsequently makes that finding, the agency should be held accountable for harm caused to the individual, in proportion to the degree of injury in a misuse of personal information, [48] and be required to improve those policies and practices to ensure only necessary information is collected moving forward.

Concluding Comments

NSW Young Lawyers as well as the CET Committee thank you for the opportunity to make this submission. If you have any queries or require further submissions, please contact the undersigned at your convenience.

Contact:

[redacted]

[redacted]

Email [redacted]

Alternate Contact:

[redacted]

[redacted]

Email: [redacted]

[48] Damon Greer, 'Privacy in the Post-Modern Era - An Unrealized Ideal' (2011) 12 *Sedona Conference Journal* 189.