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
policy@justice.nsw.gov.au

23rd August 2019

SUBMISSION

NSW DEPARTMENT OF COMMUNITIES AND JUSTICE

INQUIRY INTO ADOPTING A MANDATORY REPORTING SCHEME FOR DATA BREACHES

Genna Churches
Monika Zalnieriute
Graham Greenleaf
The Allens Hub for Technology, Law & Innovation
UNSW Faculty of Law Sydney, Australia

About Us

We are scholars researching intersections between law & technology, constitutional and administrative law, human rights and legal theory at the Allens Hub for Technology, Law and Innovation ('the Allens Hub'). Based at the UNSW Sydney Faculty of Law, Allens Hub is an independent community of scholars, which aims to enrich academic and policy debates and drive considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the Allens Hub can be found at *http://www.allenshub.unsw.edu.au/*.

Genna Churches is a PhD candidate at UNSW Law. Her thesis, 'The Evolution of Metadata Regulation in Australia: From Envelopes and Letters to URLs and Web Browsing', focuses on the access to and retention of telecommunications metadata, questioning if historical parliamentary debates and legislation of analogous technologies, such as the post and the telephone, have informed the balance between privacy protections and other social objectives in current telecommunications legislation.

Dr. Monika Zalnieriute is a Research Fellow at the Allens Hub for Technology, Law & Innovation at the UNSW Sydney Faculty of Law, where she leads an interdisciplinary research stream on *Technologies and Rule of Law*. Monika's research explores the interplay between law, technology, and politics, and focuses on international human rights law Internet policy in the digital age.

Graham Greenleaf AM is Professor of Law & Information Systems at UNSW Sydney. He has been involved in privacy issues since the mid-1970s, and is a privacy advocate, board member of the Australian Privacy Foundation, and founder of the Asian Privacy Scholars Network. He has completed numerous consultancy projects for the European Commission on data privacy. His Asian Data Privacy Laws: Trade and Human Rights Perspectives (OUP, 2014) analyses data privacy laws in 28 countries. He is Asia-Pacific Editor for Privacy Laws & Business International Report and publishes biennial surveys of the world's privacy laws. He was an invited speaker at the 25 May 2018 'launch' of the EU's General Data Protection Regulation (GDPR).

We are grateful to our colleagues for their helpful comments.

About this Submission

This submission seeks to respond to the questions raised in the call for submissions by the NSW Department of Communities and Justice's ('NSW DCJ') Inquiry into Adopting a Mandatory Reporting Scheme for Data Breaches. As scholars working at the intersection of law and technology, we are delighted to participate in this inquiry led by the NSW DCJ. In this submission, we draw upon some of the research conducted by the Allens Hub researchers to assist the NSW DCJ in their inquiry. We are grateful for the opportunity to present our views and hope this submission will assist this Inquiry. The opinions expressed in this submission are the views of the authors, and do not necessarily reflect or present the views or positions of the Allens Hub or the UNSW Law.

This submission uses the term 'notification' to mean contact with the individual/s whose data has been affected, and 'report' to mean disclosure to the NSW Privacy Commissioner. Where the individual has been 'notified', this submission is written on the assumption that there will be a corresponding 'report' to the NSW Privacy Commissioner. Later in this submission we suggest a dual threshold system, similar to that prescribed in the *GDPR*, where a minor data breach may only require a 'report' to the NSW Privacy Commissioner and not require 'notification' to the individual.

Summary of Recommendations

First, we recommend that the NSW Government should adopt a mandatory data breach notification scheme for NSW public sector agencies ('NSW NDB'). We argue such scheme is necessitated by a number of factors, including an increase in the volume of data retained; consistency with federal and international standards on data breach notification; inconsistencies between the levels of protection, particularly in relation to accessed and retained 'telecommunications data'; the application of a similar scheme for NSW government data sharing;[1] good levels of support from legislators, the NSW Privacy Commissioner, NSW Law Reform Commission ('NSWLRC') and the Department of Premier and Cabinet; and finally, an increased economic efficiency through the development of holistic and specific data protection practices based on the interrogation of data reported to the NSW Privacy Commissioner.

Second, we suggest that the NSW NDB scheme should require reporting to the NSW Privacy Commissioner and notification to the individual where unauthorised access, disclosure, or loss of data has occurred. In addition, reporting and/or notification should also be required where Information Protection Principles ('IPPs') have been breached, but only where the breach is likely to cause harm. Mandatory notification in these circumstances will serve to boost confidence in the ability of departments and data holders to handle personal information correctly and go some way to protecting an individual's right to privacy and the right to an effective remedy.[2] Reported information will also inform better data handling practices.

Third, we argue that the threshold of 'serious harm' is too high for the NSW NDB, given factors which may not be within the knowledge of the data holder, such as the particular situation of the individual; the growing ability for data to be reidentified and matched with existing data through new technologies; does not reflect the expectation of the public who are

[1] See *NSW Data Sharing (Government Sector) Act 2015* (NSW) ('NSW Data Sharing Act') s 12.
[2] *Privacy and Personal Information Protection Act 1988* (NSW) ('*PPIP Act*') s 55(2) already provides limited compensation for breaches of information protection principle/s ('IPP/s') or a privacy code of practice.

concerned with breaches of privacy (and not 'serious harm'); and does not reflect international standards such as those under the *General Data Protection Regulation* ('*GDPR*').[3]

Instead, we recommend a dual threshold system where the individual should be notified if the breach is *likely* to be a high risk to an individual's rights and freedoms. The NSW Privacy Commissioner should be notified by report in all circumstances except where the breach is *unlikely* to affect an individual's rights and freedoms. Reporting and notification should also occur where there has been a breach of IPPs which is likely to cause harm.

Fourth, we suggest that no exception be made to the requirement for reporting to the privacy Commissioner and/or notification to the individual where remedial action has been taken, no matter how successful that action has been. The failure to notify the individual could well affect their right to privacy and/or a right to an effective remedy. The failure to report to the NSW Privacy Commissioner means the information is not available to be assessed to improve data handling practices and procedures.[4]

Fifth, we propose that reports to the NSW Privacy Commissioner must contain sufficient information to enable the NSW Privacy Commissioner to advise the specific data holder on how to improve their processes, procedures and policies to prevent breaches occurring, and more broadly to aggregate the data to determine best practices across the agencies and organisations covered under a NSW NDB. The NSW Privacy Commissioner should also maintain a website with current and historical data breach notifications to ensure that parties who cannot be notified have an independent point of notification. Similarly, current and historical data should be made available to researchers focusing on improving the protection of data.

In the same vein, the notifications to the individual should contain information identifying the type of data breached, when it occurred, the remedial action taken, the success or otherwise of

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88 ('*GDPR*').
[4] We note that the *GDPR* does permit some exceptions; *GDPR* arts 33, 34.

that remedial action, any further remedial action which the Department suggests the individual should take, and an explanation of the individual's rights to seek a remedy.

Sixth, we recommend that notification to individuals should occur immediately whenever there is a high risk that their rights and freedoms may be affected by the data breach. Reporting to the NSW Privacy Commissioner should occur within 72 hours of the detection of the breach, or immediately should it become apparent that the data holder cannot quickly contact the individuals affected. This would then permit the NSW Privacy Commissioner to place notification on their website notifying individuals with this type of data held by the particular type of organisation may be at risk, and to contact the designated person.

Seventh, we recommend that the NSW Privacy Commissioner be granted powers of investigation, without the requirement of a complaint, along with the ability to fine data holders and, where appropriate, prohibit data holders from retaining certain types of information until they can demonstrate their processes and procedures are adequate to protect that information. We also recommend six monthly reporting and inclusion in the Privacy Commissioners Annual report with annual review by the Parliamentary Committee.

Eighth, we recommend that there be no exemption from reporting to the NSW Privacy Commissioner or notifying the individual if the required thresholds have been met, particularly where joint data holders are concerned. Both data holders should be required to make notifications and reports.

Finally, we suggest, that a separate inquiry assessing the privacy and data handling protections, including the possible application of the NSW NDB scheme to law enforcement agencies, be undertaken.

Submission

1. The NSW Government Should Introduce a Mandatory Data Breach Notification Scheme for NSW Public Sector Agencies

We argue that the NSW Government should adopt a mandatory data breach notification scheme for NSW public organizations (NSW NDB) for several reasons. First, it is needed to ensure the protection of personal information in NSW as more and more data is retained and stored. Second, such scheme would bring NSW in line with Australian Federal and International standards on data breach notification. Third, NSW NDB scheme is crucial to address lack of protection when NSW public organisations access 'telecommunications data' retained under *Telecommunications (Interception and Access) Act 1979 (CTH) ('TIA Act')*. Fourth, we note that mandatory data breach reporting mechanisms already exists in the context of NSW government sector data sharing, and that it should be extended to cover public sector comprehensively. Fifth, we note that there have been great levels of support for the NSW mandatory breach notification scheme with regards to Bills introduced, as well as the Recommendations made by the NSW Privacy Commissioner and NSWLRC. Finally, we suggest that the mandatory reporting scheme will increase economic efficiency and provide financial benefits to the NSW public sector.

1.1 Increase in Volumes of Generated and Retained Data Necessitates Stronger Protection

The amounts of data generated and retained about individuals in Australia have increased exponentially over the last decade, [5] and this, we suggest, necessitates introduction of stronger protection for personal data. This is especially so because some types of data retention and/or storage do not involve explicit consent of the individual. For example, the *Telecommunications*

[5] Elizabeth Coombs and Sean McLaughlan, 'Australia's Mandatory Breach Notification Regime Imminent' (2017) 150 *Privacy Laws & Business International Report* 1, 4.

(Interception and Access) Act 1979 (Cth) ('TIA') mandates the retention of certain types of data without the consent of the data subject.[6] Similarly, vehicle number plates photographed;[7] records of MAC[8] addresses;[9] and logging of MAC addresses at locations[10] are collected and stored electronically, making the data vulnerable to human error, unauthorised access, leakage, loss or public exposure. We believe the NSW Government is under a duty to act to ensure individuals are protected by adopting a NSW NDB.

1.2 NSW Data Breach Reporting Scheme Will Bring It in Line with Australian Federal and International Standards

Secondly, we suggest that the NSW NDB will bring NSW in line with the Federal scheme under the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) ('*CTH NDB*')[11] and international standards on data breach notification, and in particular arts 33 and 34 of the *GDPR*, discussed below.

1.3. NSW Organisations Are Accessing Telecommunications Data Without Legal Protection

Thirdly, we argue that such mandatory NDB scheme for NSW is crucial to address lack of protection of retained 'telecommunications data', whenever it is accessed by the NSW public sector agencies. While such data is protected by the *CTH NDB* scheme, it does not apply to the NSW public sector organisations.

---

[6] For more information about data retention scheme, see Zalnieriute, Monika and Churches, Genna, *Submission to Review of the Mandatory Data Retention Regime Prescribed by Part 5-1A of the Telecommunications (Interception and Access) Act 1979 (CTH) ('TIA Act')* (June 28, 2019). UNSW Law Research Paper No. 19-46, 2019. Available at SSRN: https://ssrn.com/abstract=3416959.

[7] <https://www.abc.net.au/news/2013-09-09/nsw-police-quizzed-over-anpr-data/4944632>; <https://privacy.org.au/policies/anpr/; https://www.stacklaw.com.au/news/criminal-law/automatic-number-plate-recognition-anpr-technology-not-underestimated/>.

[8] Media access control address, a unique identifier assigned to electronic devices capable of connecting to a 'network'.

[9] Pawned devices have their MAC addresses recorded and forward to Police; https://www.police.nsw.gov.au/safety_and_prevention/safe_and_secure/personal/media_access_control

[10] https://www.rms.nsw.gov.au/about/news-events/news/roads-and-maritime/2013/130909-travel-monitoring-bluetooth.html

[11] Amendment to the *Privacy Act 1988* (Cth).

We reason that this legal loophole is particularly acute, as more and more NSW public sector organisations are attempting to access 'telecommunications data'. For example, a recent submission by the Communications Alliance to the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') Inquiry of the Mandatory Data Retention Regime has detailed how various public organisations within the jurisdiction of the proposed NSW NDB are attempting to access 'telecommunications data' under s 280 of the *TIA Act*.[12] Examples include Bankstown City Council; Dept Fair Trading NSW; Fairfield City Council; NSW EPA; NSW Office of State Revenue; NSW Government Trade, Investment, Resources and Energy; Primary Industries NSW; Rockdale City Council; Hunter Region Illegal Dumping Squad; Liverpool City Council; Report Illegal Dumping (NSW) and SafeWork NSW. Irrespective of how many organisations have successfully gained access to telecommunications data, such data is considered sensitive personal information and is protected under the *CTH NDB* scheme.[13] Further support of the implementation of such a scheme is the requirement that telecommunications providers submit a data retention plan, demonstrating their compliance with the data retention scheme, including data protection measures — obligations missing from the requirements of recipients of this data.[14]

We argue that this gap in the law is further evidenced by the PJCIS' reports of 2015[15] and 2013,[16] both recommending the implementation of a federal mandatory data breach reporting regime due to the sensitive nature of the information retained by telecommunications providers

[12] Communications Alliance, Submission No 27 to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry of the Mandatory Data Retention Regime Prescribed by part 5-1a of the Telecommunications (Interception and Access) Act 1979 (Cth)* July 2019. <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime>.

[13] *Privacy Act 1988* s 6C(1); Telecommunications (Interception and Access) Act 1979 s 187LA

[14] Although it is noted that carriers/CSPs/ISPs have been granted exceptions permitting them to leave data unencrypted; Optus Review of the mandatory data retention regime Submission 24, 3.

[15] Parliament of Australia, Parliamentary Joint Committee on Intelligence and Security Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 2015 Recommendation 38, 299.

[16] Parliament of Australia, Parliamentary Joint Committee on Intelligence and Security Report of the Inquiry into Potential Reforms of Australia's National Security Legislation, 2013 Recommendation 42.

under data retention schemes.[17] Indeed, the *CTH NDB*[18] was prepared in response to the passage of the data retention scheme in 2015 and was seen as crucial to ensure the protection of the retained 'telecommunications data'.[19] There is no reason why NSW public sector organisations accessing such information from telecommunications providers should be treated differently and not subjected to mandatory data breach reporting.[20]

1.4. Existing NSW Legislation Already Entails Mandatory Reporting for Data Sharing

Fourthly, we note that mandatory privacy breach reporting mechanism already exists in the context of NSW government sector data sharing. In particular, s 12(2) of the *NSW Data Sharing (Government Sector) Act 2015* (NSW) ('*NSW Data Sharing Act*') states:

> If a data recipient that is provided with government sector data that contains health information or personal information becomes aware that the privacy legislation has been (or is likely to have been) contravened in relation to that information while in the recipient's control, the data recipient must, as soon as is practicable after becoming aware of it, inform the data provider and the Privacy Commissioner of the contravention or likely contravention.

However, because this legislation only applies in context of government sector data *sharing*, and not generally, we suggest that the introduction of a general NSW NDB scheme would extend and standardise protections to cover the NSW public sector comprehensively.

---

[17] Passed as an amendment to the *Privacy Act 1988* (Cth); *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth); see comments on the sensitive nature of the data in Monika Zalnieriute and Genna Churches UNSW Law, Submission No 4 to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry of the Mandatory Data Retention Regime Prescribed by part 5-1a of the Telecommunications (Interception and Access) Act 1979 (Cth)* 28 June 2019 UNSW Law Research Paper No. 19-46, 2019 Available at SSRN: https://ssrn.com/abstract=3416959.

[18] Privacy Amendment (Notification of Serious Data Breaches) Bill 2016.

[19] Many of the 47 submissions received by the AG Departments highlighted the necessity for the data breach scheme for this reason. Submissions listed here: <https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx>.

[20] Monika Zalnieriute and Genna Churches UNSW Law, Submission No 4 to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry of the Mandatory Data Retention Regime Prescribed by part 5-1a of the Telecommunications (Interception and Access) Act 1979 (Cth)* 28 June 2019 UNSW Law Research Paper No. 19-46, 2019. Available at SSRN: https://ssrn.com/abstract=3416959; Telstra, Submission 35 to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry of the Mandatory Data Retention Regime Prescribed by part 5-1a of the Telecommunications (Interception and Access) Act 1979 (Cth)* 4.

1.5. Previous Recommendations for an NSW MDBN Scheme

Fifth, we recognise the great levels of support and previous recommendations for a NSW NDB scheme. There have been previous private member Bills[21] and general support from the Labor opposition for a NSW MDB scheme.[22] In February 2015, the Report of the NSW Privacy Commissioner recommended that the *Privacy and Personal Information Protection Act 1998* (*PPIP Act)* be amended to 'provide for mandatory notification of serious breaches of an individual's privacy by a public sector agency'.[23] The Department of Premier and Cabinet echoed the calls for amendment.[24] The NSW Privacy Commissioner's Report also recommended an amendment to the Annual Reports Act 1984 (NSW) to 'require reporting of serious breaches and actions taken to address the breaches'.[25]

Moreover, in 2010, the New South Wales Law Reform Commission ('NSWLRC') recommended the inclusion of a NDB scheme within the *Privacy and Personal Information Protection Act 1988* (NSW) ('*PPIP Act*'):[26]

> (1) An agency is required to notify the Privacy Commissioner and affected individuals when personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.
>
> (2) In determining whether the acquisition may give rise to a real risk of serious harm to any affected individual, the following factors should be taken into account:
>
> (i) whether the personal information was encrypted adequately; and

[21] Privacy and Personal Information Protection Amendment (Notification of Serious Violations of Privacy by Public Sector Agencies) Bill 2017 (NSW).
[22] <https://www.itnews.com.au/news/nsw-opposition-reignites-push-for-mandatory-data-breach-laws-527080>; <https://www.itnews.com.au/news/nsw-govt-agencies-could-be-forced-to-report-data-breaches-477844> .
[23] *Report of the Privacy Commissioner under Section 61B of the Privacy and Personal Information Protection Act 1998* (NSW), 24.
[24] Ibid, 67.
[25] Ibid, 24.
[26] New South Wales Law Reform Commission, Report 127 *Protecting Privacy in New South Wales* May 2010, recommendation 9.2.

(ii) whether the personal information was acquired in good faith by an employee or agent of the agency where the agency was otherwise acting for a purpose permitted by the Privacy and Personal Information Protection Act 1998 (NSW) (provided that the personal information is not used or subject to further unauthorised disclosure).

(3) An agency is not required to notify an affected individual where the Privacy Commissioner considers that notification would not be in the public interest or in the interests of the affected individual.

(4) Data breach notification provisions should be enforced in the same manner as an IPP under the Privacy and Personal Information Protection Act 1998 (NSW).

While a similar framework could be used for the proposed NSW NDB scheme, we suggest that the threshold of for reporting recommended by the NSWLRC and encapsulated in the *CTH MDBN* is too high to meet public expectations or bring it line with the international standards.

1.6. Data Breach Regime Will Increase NSW Public Sector Economic Efficiency

Finally, we suggest that the NSW NDB will provide financial benefits to the NSW public sector through a reduction in consultancy costs for individual departments with respect to data handling practices. Under our proposed comprehensive regime, the NSW Privacy Commissioner, with sufficient data from reporting, will be able to develop a more holistic, NSW public service-centred approach to information privacy, data handling and application of IPPs.

In sum, for all these reasons, the NSW Government should introduce a mandatory data breach notification scheme for NSW public sector agencies

2. The NSW Scheme Should Require NSW Public Sector Agencies to Report Breaches Where Unauthorised Access to or Disclosure of Personal Information has Occurred *or* Where IPPs Have Been Breached

We suggest that the NSW NDB scheme should require reporting to the NSW Privacy Commissioner and notification to the individual where unauthorised access, disclosure, or loss of data has occurred. The threshold of reporting/notification should be at the *GDPR* dual threshold standard as we explain in part 3 of this submission. In addition, reporting and notification should also be required where IPPs have been breached *and* are likely to cause harm.

Mandatory notification will serve to boost confidence in the ability of departments and data holders to handle personal information correctly and protect an individual's right to privacy, including the right to an effective remedy.[27] Information reported to the Privacy Commissioner will also inform better data handling practices. Similarly, notification and reporting on IPP breaches likely to cause harm, would provide the community with confidence that their information is being handled correctly and create a deterrent for not abiding by IPPs — that the data holder may suffer reputational harm through having to notify and report that they breached the IPPs to the threshold of likely to cause harm.[28]

To increase community confidence and incentives for data holders to comply with IPPs and prevent data breaches, we suggest that notification reports should be published, including the data holders name, on a publicly accessible website. This would not only aid in notifying individuals who cannot be contacted or where contact efforts have failed, but would also become a central repository for research on how to improve data handling and protection

[27] The *PPIP Act* s 55(2) already provides for limited compensation for breaches of information protection principle/s or a privacy code of practice.
[28] Australian Law Reform Commission, Report 108, *For Your Information*, 1669-70.

practices and improve processes for those data holders who *regularly* appear on the notification list.[29]

We also suggest that mandatory notification of data breaches to the GDPR standard and IPP breaches likely to cause harm, would bring NSW in closer compliance with the *International Covenant on Civil and Political Rights* ('*ICCPR*'),[30] provide valuable external monitoring through the Information Privacy Commission NSW ('NSW IPC') and external examination by civil society and legal researchers.[31] Overall, we would like to emphasize that the right to privacy is a human right and any notification scheme must be reflective of the importance of protecting that right.

2.2. At What Threshold do Individuals Expect to be Notified?

Surveys conducted by the NSW IPC and the University of Sydney in 2017, demonstrate that NSW citizens and residents are concerned about their privacy.[32] When considering privacy breaches, respondents to the NSW IPC survey held public servants to a higher standard, reflecting that where a public sector employee has released information to a non-government organisation, legal action was the appropriate remedy. A number of other remedies, including recognition as a criminal offence were canvassed within the survey. Of course, these remedies can only occur where the individual in question is *notified* that their information has been the subject of a data breach.[33]

[29] Graham Greenleaf, 'Australia's Data Breach Notification Bill: Transparency Deficits' (2016) 139 *Privacy Laws & Business International Report* 18-19, 30 January 2016.
[30] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) ('*ICCPR*') art 17.
[31] Graham Greenleaf, 'Australia's Data Breach Notification Bill: Transparency Deficits' (2016) 139 *Privacy Laws & Business International Report* 18-19, 30 January 2016; Human Rights Council Twenty-seventh session Agenda items 2 and 3 Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development The right to privacy in the digital age Report of the Office of the United Nations High Commissioner for Human Rights 30 June 2014 A/HRC/27/37 .
[32] Information and Privacy Commission NSW, Attitudes of the NSW Community to Privacy 2017.
[33] Information and Privacy Commission NSW, Attitudes of the NSW Community to Privacy 2017, 23.

Similarly, the survey published by the Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey* in 2017,[34] demonstrated that data security and data breaches were the third greatest concern to the participants,[35] with 95 per cent agreeing that they should be told about any losses to their data by a government agency with over eight in 10 people agreeing with a mandatory data breach reporting scheme.[36] Moreover, the University of Sydney survey gave examples of what participants felt was a breach of their privacy. Eighty-two per cent of respondents confirmed that 'the sharing of a non-intimate photograph online without permission' was a breach of privacy.[37]

This threshold is lower than 'serious harm', or even 'harm' as the respondents were able to articulate that this was *an action which affected their rights*, namely, the right to privacy. We therefore suggest that the threshold for notification/reporting under NSW NDB should be equally low. As we elaborate in more detail in Section 3, the threshold should be at a similar level to that specified by the *GDPR* where reporting is always mandated unless the risk to individual's rights is *unlikely;* and notification to individual is *required* where there is a high risk to those rights.[38]

2.3. Why should NSW Citizens/Residents Expect Less Protections?

We suggest that consistency across NSW and Federal schemes would grant NSW citizens/residents protections across the majority of organisation with whom they interact. Given the NSW public sector is only bound by a voluntary reporting scheme (with the exception of *NSW Data Sharing (Government Sector) Act 2015 (NSW)*) and the private sector

[34] Jayne Van Souwe, Patrick Gates, Ben Bishop, Claire Dunning, Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2017 Report* <https://apo.org.au/node/117461>.
[35] Ibid, 4.
[36] Ibid, 16.
[37] Information and Privacy Commission NSW, *Attitudes of the NSW Community to Privacy 2017*; see also Gerard Goggin, Ariadne Vromen, Kimberlee Weatherall, Fiona Martin, Adele Webb, Lucy Sunman and Francesco Bailo, *Digital Rights in Australia* (Departments of Media and Communications, and Government and International Relations, Faculty of Arts and Social Sciences, and the University of Sydney Law School, November 2017), 17.
[38] *GDPR* arts 33, 34; see a more detailed discussion below.

largely bound by the *CTH NDB* scheme, why should NSW citizens/residents accept less accountability when they provide data to the NSW public sector?

NSW residents have every right to expect state agencies to report data breaches to least at the same level as the *CTH NDB*. However, NSW residents, and Australians in general, are still at a disadvantage compared to those covered by the *GDPR*, which specifies a lower threshold for notification. This *GDPR* standard, focussing on the measure of risk to the rights and freedoms of the individual, we suggest, would be more suitable for the NSW NDB.

3. The Threshold of 'Likely to Result in Serious Harm' is Not Appropriate

We argue that 'serious harm' sets the threshold for notification too high for the NSW NDB. We note that the *CTH NDB* sets a threshold of 'serious harm'[39] for eligible notifications, with a further exception that if remedial action is taken it is not a notifiable breach[40]. However, we argue that in an environment of under-reporting[41] and ever-increasing risks to the rights of the individual, the threshold of 'harm/serious harm' is too high.

When data holders have to measure the extent of 'harm', the full magnitude of the breach may not be readily transparent to the agency, particularly where the leaked data or unauthorised access is paired with other information from other sources, such as previously leaked information, or could be re-identified — important considerations with the increase in data matching techniques and the use of artificial intelligence.[42] Equally, the data holder may not

[39] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) s 26WE(2)(a).
[40] A number of other exemptions also apply.
[41] NSW Department of Communities and Justice, Discussion Paper, 'Mandatory notification of data breaches by NSW public sector agencies', July 2019, 8 [3.14]; Australian Government, Office of the Australian Information Commissioner, *Notifiable Data Breaches scheme 12-month insights report*, 13 May 2019, 4.
[42] See, eg Natasha Lomas, 'Researchers spotlight the lie of 'anonymous' data' Tech Crunch (Online) 24 July 2019 <https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/>.

be fully cognisant of the particular sensitivities and circumstances of the individual and therefore may be unaware of the level of harm which could occur.[43]

Instead, to encourage best practice in information and data handling techniques, procedures and policies, we argue that mandatory reporting and notification should be at a lower threshold irrespective of remedial action.[44] We suggest the best measure is the likely effect on an individual's rights — right to privacy, freedom of expression and in extreme cases, the right to life. For example, the *GDPR* requires notification of the individual where the data breach is likely result in a high risk to the individuals' rights and freedoms.[45] However, the *GDPR* mandates reporting of *every* breach to the supervisory authority 'unless the personal data breach is *unlikely* to result in a risk to the rights and freedoms of natural persons'.[46] We therefore recommend a dual threshold system which mandates reporting to the NSW Privacy Commissioner for all breaches except those which are *unlikely* to pose a risk to the individuals' rights and freedoms, and notification to the individual where there is a high risk to those rights.

When assessing the *CTH NDB*, the Senate Standing Committee for the Scrutiny of Bills commented that the scheme had too many exceptions to the notification of the individual, resulting in a scheme which interfered with the right to privacy.[47] A dual threshold reporting scheme based on the *GDPR* would recognise the interference with the rights of the individual, providing notification where there is a high risk to those rights and freedoms, and mandatory reporting to the Privacy Commissioner in all other circumstances except those which are unlikely to result in a risk. These thresholds should operate irrespective of any remedial action.

[43] For example, a history of domestic violence.
[44] Under the CTH NDB scheme, if remedial action has been taken, then the individual is not required to be notified.
[45] *GDPR* art 34.
[46] *GDPR* art 33.
[47] Parliament of Australia, Senate Standing Committee for the Scrutiny of Bills, *Alert Digest*, 8/2016, 30.

3.1. If 'serious harm' is the threshold then it should be defined in legislation

Whatever threshold is determined by Parliament, it should be explicitly defined within legislation. Without a defined standard, data holders who do not report/notify data breaches or breaches of IPPs likely to cause harm, within time or at all, cannot be measured.

3.2. Factors to be considered when assessing a data breach should be provided

Whatever standard is determined and defined in the legislation, examples and factors to be considered should be prescribed in the legislation. It should also be made clear that the purpose of the Act is to encourage reporting and notification where appropriate — meaning that where there is doubt that the requisite threshold has been met, decisions should be weighed in favour of notification/reporting.

We argue that just as data and information is critical in providing services to customers, clients and government, the data generated though reporting and/or notification will aide improvements to the security of personal information/data.

4. Legislation Should Require Reporting, Regardless of Remedial Action

We recommend that all data breaches reaching the *GDPR* threshold of high risk to an individual's rights and IPP breaches likely to cause harm, irrespective of remedial actions, should be reported to the Privacy Commissioner and the individual notified.[48] Further, reporting to the Privacy Commissioner should occur where there has been a lesser data breach but not one which is unlikely to affect an individual's rights, again, regardless of remedial action taken.[49]

This will ensure the individual is notified at the appropriate *GDPR* threshold, going some way to satisfying the opportunity of providing an effective remedy to the breach of privacy.

[48] *GDPR* art 34.
[49] *GDPR* art 33.

Notification permits the individual who is aware of their own particular sensitivities, to take remedial action. Similarly, as discussed in part 2 of this submission, the public has expressed a right to know when their privacy has been breached.

We argue that information reported to the Privacy Commissioner about the type/s of remedial action/s taken, and their effectiveness could improve the overall system giving indications as to which remedial actions work and the timeframes within which they must be applied.

The examples provided in the NSW NDB Discussion Paper at paragraph 4.15 exemplify why these situations, despite the subjective success of remedial action, should be reported. Both examples are direct results of human error but are equally preventable through processes and policies. For example, personal information could be prohibited from being accessed through mobile devices. Similarly, where personal information is being sent, there are ways to isolate the information until the sender has verified that the correct party has received the information.[50] If these incidents are not reported, the Privacy Commissioner cannot provide guidance on how to minimise the occurrence of human error-based breaches.

Human error accounted for 35% of breaches triggering a mandatory notification under the CTH NDB scheme. The types of human error are shown in the table below:[51]

[50] As simple as the provision of a password upon confirmation of receipt of the information, or the variety of solutions provided by Outlook and other MS Office365 products.
[51] Australian Government, Office of the Australian Information Commissioner, *Notifiable Data Breaches scheme 12-month insights report*, 13 May 2019 <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/#human-error-breaches-and-system-faults>.

Figure 6 — Human error breaches—all sectors, from 1 April 2018 to 31 March 2019

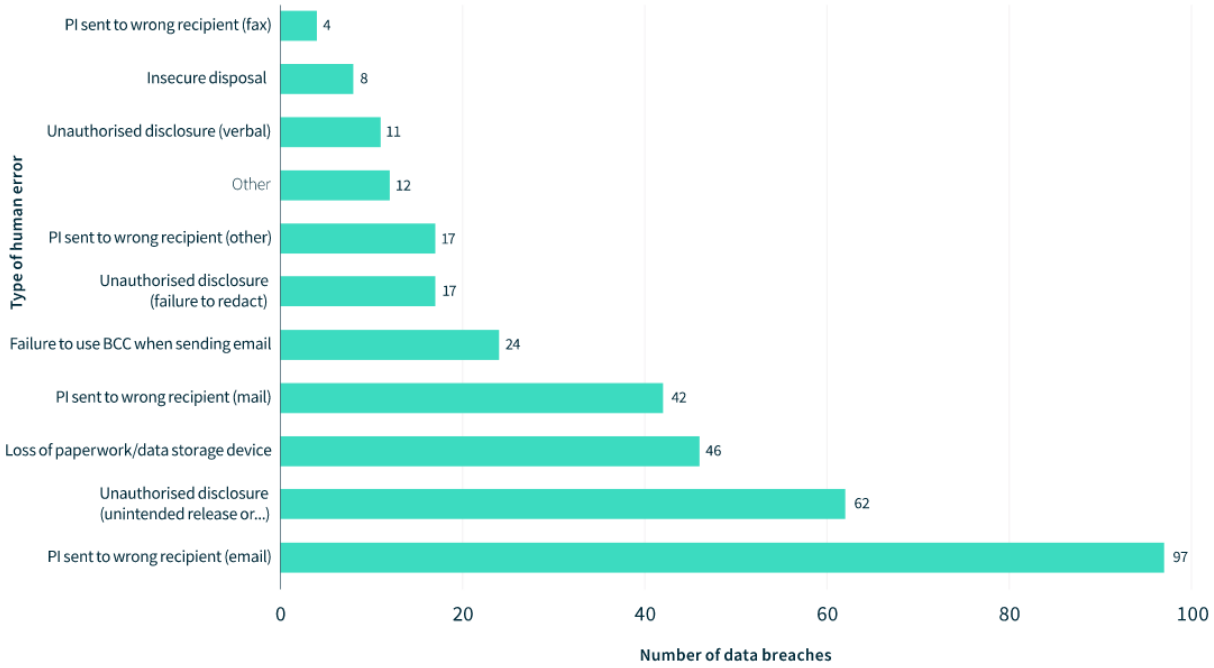

Figure 6: Long text description

Federally, this type of information is being used to improve processes.[52] NSW has the opportunity to learn from the *CTH NDB* scheme to develop a comprehensive system which strives for constant improvement in data handling. Further, this opportunity may present cost savings through a reduction in consultancy costs for individual departments with respect to data handling practices. Instead, a more holistic, NSW public sector specific, approach could be developed by analysing the data from reports and/or notifications.

[52] Australian Government, Office of the Australian Information Commissioner, *Notifiable Data Breaches scheme 12-month insights report*, 13 May 2019 <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/#learnings>.

5. Information Required for Reports to the Privacy Commissioner and/or Notifications to the Individual should be described in Legislation

We recommend that the information reported to the Privacy Commissioner under the NSW NDB should be sufficient to recognise the dual purpose of reporting. The primary purpose being to notify affected individuals to minimise the risk to their rights and freedoms and/or provide a right to an effective remedy. The secondary purpose being to provide information to the Privacy Commissioner to aide improvements to data handling/data protection and adherence to IPPs, through the interrogation of the information received.

In addition to any information which identifies the parties affected so they can be notified/followed up with, we recommend the data reported to the Privacy Commissioner should include: the types of breach/es (ie breaches of IPPs likely to cause harm or unauthorised data access, et cetera); the types of data affected; the frequency of breaches (if more than one); how the breach was detected; the timeframe from breach to detection; relevant technical data from an ICT perspective; an assessment on how the breach affects the rights of the individual; remedial action taken and its success or otherwise; recommendations on further remedial action and detailed information on how the data holder is going to change policy, processes or procedures to prevent breaches in the future, including an assessment of the failures which caused the breach.

We recommend that the data be sufficient for the Privacy Commissioner to post information about data breaches on its website so that individuals affected who cannot be contacted by other means have a point of notification beyond the details held by the data holder. This repository would also aide research and provide individuals with an indication on the ability of the data holder to protect data.[53]

[53] Graham Greenleaf, 'Australia's Data Breach Notification Bill: Transparency Deficits' (2016) 139 *Privacy Laws & Business International Report* 18-19, 30 January 2016.

Information provided to the individual should include a description of the type of data in question; the type of breach, (i.e. unauthorised access, et cetera); a description of the remedial action taken and how successful that action has been/could be. The notification should also provide an indication if there is a further remedial action the individual should take; any further rights they may have under *PIPP Act* or other Acts; a reassurance that the Department is assessing best practices to ensure it does not happen again, and confirmation that this incident has been reported to the Privacy Commissioner.

6. Notification Timeframes

We recommend that when the data holder is reporting to the Privacy Commissioner, the *GDPR* standard of 72 hours[54] should apply. Where the data breach has a high risk of affecting an individual's rights, notification should be immediate.[55] However, it is appreciated that contacting the individual/s affected may not be a straightforward process. Data holders may only have a postal address for the individual affected which would cause delay in contact. This is another reason why we recommend the Privacy Commissioner establishes a regime for publishing notifications regarding breaches on their website. Individuals will have an up-to-date and central point of contact which they can periodically check to ensure their data is secure. [56] For the individual, contact within 72 hours could still permit sufficient time to take remedial action to prevent adverse effects.

There may be situations where the data holder is unaware that the data breach has occurred, or is perhaps unaware of the scope of the data breach, in which case reporting will be some time after the 72 hours has expired, but we argue that valuable information about the processes, policies and mechanisms in place within the data holders organisation will still be gained from late reporting.

[54] GDPR art 33.
[55] GDPR art 34.
[56] Graham Greenleaf, 'Australia's Data Breach Notification Bill: Transparency Deficits' (2016) 139 *Privacy Laws & Business International Report* 18-19, 30 January 2016.

7. NSW Privacy Commissioner Additional Powers

We propose that the Privacy Commissioner requires sufficient powers to conduct annual and spot reviews and investigations into processes, policies and procedures implemented by data holders to ensure their compliance with IPPs, their ability to detect data breaches, and make the relevant reports/notifications and investigations. The IPCNSW may need to become more ICT focused to ensure the currency of best practices from an ICT perspective.

We argue that Privacy Commissioner requires powers to investigate whistle-blower claims regarding data handling practices of data holders. This would also require the inclusion of the Privacy Commissioner in the public interest disclosures regime.[57]

Data is a valuable commodity, with some putting its value higher than oil.[58] Holding data is a tremendous responsibility, and the Privacy Commissioner *must* have commensurate powers.

7.1 Fines and/or Penalties

While we agree that monetary penalties can serve as a deterrent, we argue that fines should go directly to the IPCNSW to assist with funding and further investigation of privacy/data breaches. Some data protection authorities in Europe are considering a similar model where at least a portion of the fine is retained by the agency issuing it.[59] In NSW, fines should be wholly retained by the IPCNSW.

We suggest that a hybrid type system of deterrent is a better model. A hybrid system would be able to issue fines but also have the capability to prohibit certain types of data from being retained by the data holder. For example, the Privacy Commissioner may investigate unauthorised access to data through a hacking incident. That investigation may reveal

[57] Elizabeth Coombs and Sean McLaughlan, 'Australia's mandatory breach notification regime imminent' (2017) 150 *Privacy Laws & Business International Report* 1, 4.
[58] <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.
[59] Information Commissioner's Annual Report and Financial Statements 2018-19 Report Presented to Parliament pursuant to Section 139(1) of the Data Protection Act 2018 and Section 49(1) of the Freedom of Information Act 2000 and Accounts Presented to Parliament pursuant to paragraph 11(4) of Schedule 12 to the Data Protection Act 2018.Ordered by the House of Commons to be printed on 8 July 2019.

insufficient processes and procedures in place to protect the data, by which the Commissioner could issue a fine. The Commissioner may find that the breached data contained additional information which was not required by the data holder and should have been deleted. The Privacy Commissioner could then issue a prohibition notice that the data holder is prohibited from retaining that type of data into the future. Alternatively, where monetary penalties have not served as a deterrent or have not motivated a data holder to take preventative and protective measures, we recommend that the Privacy Commissioner should issue a temporary prohibition notice that the data holder is prohibited from retaining certain types of data for a period of six months or until the data holder can demonstrate that its systems, policies and procedures are sufficient to protect that data.

A hybrid system could also work particularly well in a government department situation where the incentive to change systems, policies and procedures may not be triggered by a monetary penalty.

An additional approach which could have a very strong dissuasive effect is to provide for statutory damages to be payable, without need for proof of actual damage, to any person whose data was involved in a data breach which is of sufficient seriousness to be required to be notified to the individuals concerned. One of the significant problems with data breaches is that individual may learn that their data was breached, and they may have suffered loss, but there is no way by which they can prove that the breach caused the loss. Korea has implemented such a statutory damages scheme with a maximum amount of the equivalent of US $3,000, where at least negligence on the part of the data controller can be established.

7.2 Oversight and Reporting

We recommend that the Privacy Commissioner prepare six-monthly reporting on the NDB reports received, relevant analysis of them and any investigations undertaken or on going. This should be supplemented by inclusion in the Privacy Commissioners Annual report and annually reviewed by the Parliamentary Committee. This will enable findings of deficiencies within existing legislation, as flagged by the Privacy Commissioner, to be quickly assessed and addressed.

We suggest the NSW MDB Act should require the Auditor General to conduct a review across the NSW public sector of the implementation of the NDB scheme and the reports of the NSW IPC.

8. Exemptions from the Requirement to Notify Individuals and the NSW Privacy Commissioner

We recommend that there be no exemption from notifying the Privacy Commissioner or the individual if the required thresholds have been met. If joint holders of data as subject to the same data breach, then both should report to the Privacy Commissioner and the individual, despite an exception existing in the *CTH NDB*. For example, there may be nuances in the information which one data holder observed and the other data holder did not. Similarly, there should not be collusion in reporting to ensure that the facts are not 'sanitised' for consistency between the data holders. Open and honest reporting should be expected, if not demanded as, after all, data protection is a vitally important goal that all departments and organisations should be working towards.

We suggest that public expectations of notification extend to law enforcement agencies, and given the sensitivity of data held by such agencies, there should be no prohibition on reporting from law enforcement agencies. We recommend that a separate inquiry assessing data handling practices, and the potential for applying IPPs and NDB schemes to law enforcement bodies should be undertaken.

8.1 Human Rights and Overall Data Protection Benefits

We endorse the importance of notifying the affected individual. Swift and detailed notification can prevent or minimise the effect on rights and freedoms caused by data breaches and harm caused by IPP breaches. In addition, a NDB scheme provides the individual with the fundamental right to an effective remedy[60] in response to an infringement of other human

[60] *ICCPR* Art 2.3.

rights, such as the right to privacy.[61] This means that there cannot be an exception to notification because remedial action has been taken. The individual expects to be informed, as discussed in part 2 of this submission, and is entitled to be informed given the human right to an effective remedy. Without notification this right is infringed.

Conclusion

As this submission has discussed, a mandatory data breach notification scheme is not new or novel. Best practice sees NDB schemes implemented concordantly with IPPs or other data minimisation and protection methods. The current disparity between NSW laws and *CTH NDB* protections must be resolved.

Our suggestions above are based on the best elements from the *GDPR* and the *CTH NDB*, informed by our backgrounds and research in rule of law, human rights protections, and information communications technology, providing a framework for the New South Wales Department of Communities and Justice to build a mandatory data breach reporting scheme which will set the standard for other States, and potentially the Federal Government.

Technology has changed the way we conduct business, gather information and provide services both in the private and public sectors. We stand on the precipice of greater and faster changes based on new and evolving technologies. It is vital that we implement the very best protections within the realms of our current understandings to provide the best opportunity of being prepared for those changes to come. There is no doubt that a mandatory data breach reporting scheme, of the calibre we have described, fits that bill.

Further, we argue that NSW has a larger responsibility in this field. As Michael Kirby orated at the launch of Privacy Month in 2016,[62] NSW has led the way on privacy protections from the first state-based Privacy commissioner in 1975, through to the revolutionary 2016 report from the Standing Committee on Law and Justice 'Remedies for the serious invasion of privacy in New South Wales', recommending a statutory tort for the invasion of privacy. With Sydney

[61] *ICCPR* Art 17; *Universal Declaration of Human Rights* Art 12.
[62] Michael Kirby, Privacy Awareness Month <https://www.ipc.nsw.gov.au/pam-2016> 17.

being home to prominent technology businesses such as Google and Facebook, and a leading-edge technology sector, it seems only natural that legislation relating to freedoms, rights and protections potentially impinged by the ubiquity of technology would be developed here.

New South Wales can and should lead the way on a revolutionary mandatory data breach notification scheme.
