Submission to Privacy Act Review Issues Paper

Institute for Cyber Investigations and Forensics, University of the Sunshine Coast

Executive summary

The Institute for Cyber Investigations and Forensics (**the Institute**), University of the Sunshine Coast, welcomes the opportunity to contribute to the Privacy Act Review. The Institute is comprised of experts in privacy and cyber security, data breach preparedness and response, identity theft and protection, and digital forensics. These diverse areas of expertise have been brought to bear on the issues raised by the Issues Paper.

This submission is informed by an understanding of current legal and regulatory frameworks and their objectives, as well as the practical reality of what happens "on the ground" in the world of privacy and cyber security. The intention is to provide a perspective that integrates considerations arising for policy-makers, businesses and individuals.

The Terms of Reference identify a broad range of areas for discussion. This submission focuses on two of those areas:

1. The current exemptions under the *Privacy Act 1988* (Cth) (**the Act**) – particularly the small business exemption – and whether these exemptions should be removed or amended.
2. The impact and effectiveness of the notifiable data breaches scheme (**NDB scheme**).

Current exemptions under the Act

The current exemptions limit the effectiveness of the Act, as most Australian organisations are exempt from any substantive privacy obligations. Organisations increasingly rely on the collection and use of personal information in the course of their activities, and there ought to be minimum standards to which they adhere. The poor handling or misuse of personal information poses the same risks to individuals regardless of the size or nature of the organisation that failed to secure it. Moreover, the primary obligation imposed by the Act – compliance with the Australian Privacy Principles (**APPs**) – provides a reasonable degree of flexibility; as a form of principles-based regulation qualified by considerations of reasonableness and practicability, the APPs can be adapted to the circumstances and activities of entities of different sizes.

That said, the sudden expansion of the Act to include a broader range of entities may not, on its own, result in a significant improvement in privacy practices. There is evidence to suggest that entities currently regulated under the Act have struggled to meet the obligations imposed by the APPs. If the Act were extended to include previously exempt organisations, such as businesses with a turnover of $3 million or less, it is not clear that these entities would have the expertise or resources to significantly enhance their current privacy and cyber security practices. Before expanding the operation of the Act to additional entities, therefore, there first needs to be a realistic appraisal of these entities' capability to comply with the Act, and to protect the personal information they hold from the sophisticated cyber security threats they current face.

Secondly, there needs to be an assessment of the role of government in assisting these entities to develop their privacy and cyber security capabilities. Thirdly, it would be crucial to consider whether these newly regulated entities would also be required to comply with the NDB scheme, which currently applies to all APP entities. As discussed below, expanding the operation of the NDB scheme in its current state may not necessarily serve the interests of either individuals or business.

Impact and effectiveness of the NDB scheme

The NDB scheme has increased awareness of the importance of personal information security among both organisations and consumers. However, the current law could be better geared towards achieving its primary goal: protecting individuals from identity theft and other harms associated with the compromise of personal information.

The current threshold for notification is ambiguous and any unauthorised access to or disclosure of personal information is potentially notifiable. Entities that are risk-averse or inexperienced in applying the scheme are in effect encouraged to adopt an approach of "when in doubt, notify," particularly since their obligations to impacted individuals end at the point of notification, and they are not responsible for any harm caused by unnecessary or inadequate data breach notices.

As a result, individuals are receiving notifications for data breaches that do not present a likely risk of serious harm. This risks causing notification fatigue (desensitising individuals when more serious data breaches occur). In other instances, individuals are not receiving practical or accurate advice on how they can protect themselves from personal information misuse. This creates additional anxiety and harm for individuals as they attempt to secure their personal information without an adequate understanding of the steps they need to take. This typically involves spending hours trying to contact various organisations and institutions in an effort to secure their personal information and accounts.
These problems are likely to be further accentuated if the NDB scheme is extended to small businesses and other entities that lack the resources or expertise to properly assess and notify data breaches.

There are several possible ways to improve the effectiveness of the NDB scheme. Options for reform include:

1. Uplifting the maturity of the response environment so that there are fewer tasks for impacted individuals to perform.
2. Providing clearer guidance on the threshold for notification and the types of personal information that may require notification.
3. A more active role for the regulator in assisting organisations to determine whether notification to individuals is necessary.

A final observation is that the proliferation of notifiable data breaches and the difficulties experienced by some organisations in complying with the NDB scheme suggest a lack of compliance with the APPs. Greater emphasis needs to be placed on APP compliance and on taking enforcement action when organisations breach the APPs. It is just as important to hold organisations to the standards required by the Act as it is to require data breach notification or to introduce new causes of action for individuals.

1. Current exemptions under the Act

The current exemptions to the *Privacy Act 1988* significantly limit the effectiveness of the Act. This submission will focus on the small business exemption. Many of the key arguments relating to the employee records and political parties exemptions were already addressed in Australian Law Reform Commission's (**ALRC**) 2008 report on Australian privacy law.[1] Both exemptions should be removed for the reasons identified by the ALRC, and particularly since the personal information collected by both employers and political parties can include "sensitive information" – that is, information requiring a level of protection beyond that afforded to other types of personal information, due to the adverse consequences that can follow from the mishandling of such information.[2]

[1] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008).
[2] *Privacy Act 1988* (Cth), s 6(1) (definition of 'sensitive information') ('*Privacy Act*'); Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (July 2019) 28 [B.141].

1.1. Small business exemption

By exempting businesses with an annual turnover of $3 million or less, the Act exempts the overwhelming majority (a recent estimate suggested 94 per cent) of Australian businesses from compliance with the APPs or the NDB scheme.[3] While it is reasonable and necessary to impose obligations flexibly on businesses depending on their size, the current "all or nothing" approach in which businesses are either entirely exempt from the Act, or are otherwise required to comply with the APPs and the NDB scheme, does not strike the right balance. The $3 million threshold is arbitrary; businesses' privacy obligations are determined by their turnover rather than by the nature of the personal information they handle or the activities they engage in.

Exempt businesses are not required to inform individuals of the collection of their personal information (APP 5), or to obtain individuals' consent to the collection of their personal information (APP 3). Where businesses do obtain consent to collect personal information for one purpose, they can use the personal information for a secondary purpose without notifying the individual or obtaining their consent (APP 6). They can also collect personal information when doing so is not reasonably necessary for the business' activities (APP 3). Exempt businesses are not required to collect personal information directly from individuals where reasonable to do so (APP 3), give individuals access to the personal information held about them (APP 12), or protect their personal information from misuse, interference and loss, or from unauthorised access, modification or disclosure (APP 11). They can also disclose personal information overseas without taking reasonable steps to ensure that the recipient will comply with the Act or any other privacy standards (APP 8).

When there is unauthorised access to or disclosure of personal information resulting in a high risk of misuse, there is no obligation to notify individuals so that they can take steps to protect themselves from identity theft (the NDB scheme). In effect, small businesses are not required to adhere to practices that are consistent with the

[3] Explanatory Memorandum, *Privacy Amendment (Notifiable Data Breaches) Bill 2016* (Cth) 38 [184].

responsible collection and handling of personal information, despite the fact that they may be collecting many of the same types of personal information as APP entities – names, dates of birth, residential and email addresses, as well as types of personal information that lend themselves to misuse more readily, such as payment details, driver's license numbers and passport numbers.

There are several cogent arguments for requiring businesses, regardless of their size and turnover, to comply with the Act, particularly the APPs. Many of these arguments are identified in the Issues Paper and include:

1. The arbitrary nature of the $3 million threshold; businesses' privacy obligations are determined by their turnover rather than by the nature of the personal information they handle or the activities they engage in.
2. The increasing reliance on the collection and use of personal information by businesses, including small businesses.
3. The lack of similar exemptions under comparable privacy regimes.
4. The complexity and uncertainty created by exempting businesses based on their turnover, while also creating exceptions to the exemption, such as for health service providers and organisations that trade in personal information.
5. Community expectations with respect to privacy.[4]
6. Organisations with lower privacy and cyber security protections may become more attractive targets for criminals and scammers.

There are two other relevant considerations, which go to the purpose and operation of the APPs. Firstly, the APPs describe practices that are consistent with the responsible handling of personal information. In other words, they describe practices that an entity, giving due consideration to the importance of the proper handling of personal information, could be expected to adopt. For example, entities should not collect personal information except where reasonably necessary for its functions or activities (APP 3), and entities that collect personal information for one purpose should not be used for a secondary purpose except in limited circumstances (APP 6).

[4] See, for example, Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020* (September 2020) 60.

Related to this, as a form of principles-based regulation, the APPs describe objectives rather than specific compliance requirements. They are less focused on box-ticking measures and are more adaptable to the circumstances of each entity.[5] This is reflected in the language of the APPs, which are typically qualified by considerations of "reasonableness" and "practicability"; that is, organisations are only required to take such measures as are reasonable or practicable in the circumstances. This would presumably include consideration of an organisation's resources and the types of personal information it collects. Considerations of reasonableness and practicability extend to the implementation of practices, procedures and systems so as to comply with the APPs, notifying individuals of the purpose and circumstances surrounding the collection of their personal information, and taking steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

That said, while these are persuasive reasons to extend the application of the Act to small businesses, consideration needs to be given as to how this will work in practice.

1.2. Expertise and resourcing

The first issue to consider in requiring small businesses to comply with the APPs (and potentially the NDB scheme) is one of expertise and resourcing. Many small businesses lack the resources or know-how to become APP compliant. While small businesses can avail themselves of various resources easily enough, including standard form privacy policies and procedures available online, implementing the principles contained in these documents and adopting practices consistent with a privacy by design approach requires much more than simply "signing off" on generic forms that do not reflect the actual reality of a business' practices.

[5] Mark Burdon, Jodie Siganto and Lizzie Coles-Kemp, 'The Regulatory Challenges of Australian Information Security Practice' (2016) 32(4) *Computer Law & Security Review* 623, 626.

A truly responsible approach to privacy requires an organisation to actually understand how to manage personal information and embed best practices in its operations. These involve practical steps, such as training staff in how to and how to collect and handle personal information, implementing appropriate cyber security (and physical security) measures to prevent unauthorised access to documents, workplace systems and employee accounts, having steps in place to respond to adverse privacy and cyber security events, and undertaking privacy impact assessments to assess the privacy impacts of new projects. If the scope of the Act and the APPs are expanded to include small businesses, and nothing further is done to improve businesses' understanding of privacy issues or to enhance the cyber security posture, there is a high likelihood that such reforms will be little more than tokenistic gestures. The result will simply be the creation of more meaningless paperwork for businesses.

There are indications that not all entities currently regulated by the Act (primarily federal government agencies and businesses with an annual turnover in excess of $3 million) are APP compliant. In the context of data breach notification, the Office of the Australian Information Commissioner (**OAIC**) has indicated that some APP entities have not demonstrated an adequate understanding of their ICT environment, including the types of personal information they retain and where, and how they protect personal information from misuse, loss and unauthorised disclosure. This lack of understanding and preparation suggests non-compliance with APP 1 and APP 11.[6] These APPs require, respectively, that entities take reasonable steps to implement practices, procedures and systems to ensure they comply with the APPs, and that they take reasonable steps to protect personal information they hold from misuse, interference loss, and from unauthorised access, modification or disclosure.

More broadly, the implementation of Australia's NDB scheme is arguably indicative of relatively low levels of compliance; one of the expected outcomes of the scheme

[6] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: January–June 2020* (31 July 2020) 7.

was to provide APP entities with incentives to improve their security measures in line with APP 11.[7] In other words, the new law aimed to improve compliance with a law that had already been in force for the better part of two decades. Indeed, the use of NDB laws is primarily a product of legal developments in the United States, a jurisdiction that does not have in place a comprehensive privacy regime such as that set out in the APPs. The introduction of a NDB scheme in Australia highlights the failure of organisations to meet the standards imposed by the APPs.[8] The scheme, while also directed at mitigating identity theft, attempts to incentivise organisations to meet the information security requirements under APP 11 by requiring them to notify the OAIC and impacted individuals when data breaches occur. Given this has been the outcome when applying the APPs to organisations with an annual turnover in excess of $3 million, there is reason to be sceptical about expanding the operation of the Act to small businesses without due consideration for their ability to implement the APPs.

1.3. Compliance with the notifiable data breaches scheme

Following from this, it is necessary to consider whether small businesses would also be required to comply with NDB scheme. Unless changes were made to the application of Part IIIC (which contains the NDB scheme), amending the definition expanding the definition of "APP entity" to include businesses with a turnover of $3 million or less would also make those businesses subject to the scheme. Consequently, if a small business experienced a data breach that was likely to result in serious harm to the impacted individuals, they would be required to notify those individuals and the OAIC of the breach. While on its face, this may appear reasonable, complying with the scheme can be complicated and expensive.

A small business that experienced a cyber attack, for example, would be required to harness the requisite technical expertise to assess the existence and extent of any

[7] Explanatory Memorandum, *Privacy Amendment (Notifiable Data Breaches) Bill 2016* (Cth) 54-55 [266]-[267].
[8] Mark Burdon, Bill Lane and Paul von Nessen, 'Data Breach Notification Law in the EU and Australia – Where to Now? (2012) 28(3) *Computer Law & Security Review*, 296, 297, 302.

data breach. The business would then need to assess whether the data breach was likely to result in serious harm to impacted individuals, if practicable, within 30 days. This is despite the business likely having no experience in assessing the harm caused by the compromise of various combinations of personal information. If the business deemed serious harm likely, it would then need to prepare a notification for both the OAIC and for impacted individuals as the breach would become an "eligible data breach." As part of the notice to individuals, the business would be required to provide advice on the steps individuals should take to protect themselves from the misuse of their personal information (again, despite having no expertise or experience in the matter).[9] The business may also have follow-up queries or complaints by customers.

Not only would this process impose potentially excessive costs on businesses, but it may do little to achieve the aims of the NDB scheme – if anything, it may undermine the scheme's effectiveness. There are several reasons for this. Firstly, organisations without the resources to manage privacy and cyber security effectively will likely fail to detect or notify data breaches in many instances. Where organisations identify a data breach has occurred, they may assess the breach incorrectly, either failing to notify individuals or proceeding to notification where this is no serious risk of harm.

The latter scenario may be seriously detrimental to the effectiveness of the scheme, as it will result in notification fatigue; the more notification individuals receive, particularly where the notifications do not identify a serious risk of harm, the less emphasis and attention individuals attribute to subsequent notifications. Consequently, when individuals receive notifications for minor data breaches, they are more likely to ignore notifications that require them to take steps to protect their personal information from misuse. In the United States, for example, a 2012 study found that 36 per cent of customers who received a data breach notification thought it was junk mail. The research findings also indicated that, over time, a

[9] *Privacy Act*, s 26WK(3)(d).

smaller proportion of customers viewed a data breach notification as an important notification.[10]

Another risk is that businesses will provide poorly worded notifications that do not identify clearly the personal information compromise or provide clear advice on the steps individuals should take to protect themselves from harm. This in itself can cause additional and unnecessary harm. Receiving notification of a data breach creates stress and anxiety for individuals. This is amplified when those individuals are unsure what personal information was involved, what risks they face, or the steps they should take to protect themselves. In fact, most individuals who receive a data breach notification do not ultimately experience financial loss, but their process of monitoring credit, closing accounts, implementing additional security measures, and communicating with organisations and institutions with which the individual holds accounts involves a significant amount of stress and time.[11] According to IDCARE, Australia's identity and cyber security community support service, around half of the individuals to reach out to their service following a breach notification experience psychosomatic impacts from such events.[12]

The problems identified above have already become evident in the operation of the NDB scheme, even with its scope being restricted to the current definition of APP entities. The OAIC has referred to the need for "maturity" to develop among organisations in assessing the risk of harm resulting from a data breach, and has referred to instances where organisations have proceeded to notification despite there not being a likely risk of serious harm.[13] On some occasions, entities appear

[10] Ponemon Institute, *2012 Consumer Study on Data Breach Notification* (June 2012) 8 <http://www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf>.
[11] Emily Matta, 'Kansans at Risk: Strengthened Data Breach Notification Laws as a Deterrent to Reckless Data Storage' (2019) 67(4) *University of Kansas Law Review*, 823, 840.
[12] Coyne, A, 'The human factor: the untold impact of data breaches", IT News, May 17, 2016 https://www.itnews.com.au/news/the-human-factor-the-untold-impact-of-data-breaches-419522
[13] Office of the Australian Information Commissioner, *Notifiable Data Breaches Scheme 12-month Insights Report* (May 2019) 8.

not to have undertaken an appropriate assessment of the data breach or even determined the nature and extent of the breach before proceeding to notification.[14]

Part of the reason for these problems lies in the current structure of Part IIIC, and ways to improve this are discussed below. Nevertheless, if the entities presently bound by the APPs and the NDB scheme are struggling to apply the provisions in a manner consistent with the scheme's objectives or the regulator's expectations, it is difficult to see how organisations with fewer resources and no pre-existing privacy obligations will do any better.

1.4. Proper allocation of resources and responsibilities

Before extending the application of the Act to include small businesses, there is also a broader question to consider: where should responsibility for privacy compliance and cyber security lie? While there are strong merits to imposing at least some privacy obligations on small businesses (as outlined above), there is a need to be realistic about the capabilities of individual entities to uplift their privacy and cyber security preparedness – particularly in an environment where larger organisations have struggled. The reality is that many organisations do not have the resources or expertise to protect themselves from the sophisticated cyber threats they currently face. These threats include credential stuffing, brute force attacks, spoofing and spear-phishing, and network and device update vulnerability exploits.

There is a legitimate and necessary role for government to play in this arena, both in terms of assisting organisations to meet the legal standards imposed upon them, and in responding to and mitigating cyber security threats through entities such as the Australian Cyber Security Centre. The government has access to more intelligence about potential and developing threats, and greater ability to respond to these threats than any individual organisation. The government also has the capacity to provide an overarching level of cyber security support and response capability

[14] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: January–June 2020* (31 July 2020) 7.

that cannot be replicated by individual organisations. Delegating responsibility to individual entities is likely to result in inconsistent standards (and the inconsistent application of legal standards), leading to vulnerabilities in supply chains, and ultimately weakening the entire cyber security environment. The interplay between cyber and privacy cannot be ignored and will almost increasingly become entirely intertwined. A regulatory imposition originating from one part of government, must be considered in terms of regulatory compliance aid and support from another. This requires a systems approach, and one that advances beyond the simple completion of an online form. The 'system' and its many participants must collectively share and benefit from the insight. Australia is well away from this outcome. Government has occupied an increasing position that advances the need to share and report, but with limited reciprocal benefits in return. The Report Cyber (cyber.gov.au), scamwatch and the Office of the Australian Information Commissioner's reporting forms are all examples of these. This is far from being optimal and is likely to place pressure on a growing divide between those entities that find themselves better connected with Government and those many more organisations that are very distant from such relationships. It is also of limited value. It is one thing to not advance information and insights that can practically assist those seeking to prevent and respond because "proceedings may be afoot" or its "imprudent to discuss current investigations" so as to "not prejudice a matter before the courts", but it is entirely different when less than 0.1 percent of such matters actually are investigated and do result in criminal trials of accused. Put simply, if government was to contemplate additional reporting and compliance burden for a growing regulated entity list, it must first address and implement improvements on how it will support those regulated entities with the insights and practical measures to assist with their compliance. A government that merely knows is of no good to the people it governs. There is a growing risk of this within a privacy and cyber security context.

2. Impact and effectiveness of the NDB scheme

There is no doubt that the introduction of the NDB scheme has had some very positive impacts. The scheme has encouraged organisations to improve their privacy and cyber security practices to reduce the likelihood of data breaches occurring, and to develop data breach response plans. The scheme has also assisted individuals impacted by data breaches; when they are informed of the unauthorised access to, or disclosure of, their personal information, individuals are able to take steps to protect themselves from the misuse of that information.

More broadly, the increased public awareness of data breaches and the importance of personal information has contributed to a broader conversation about the responsibility of organisations to protect the personal information they hold from unauthorised access and misuse.

2.1. Maturity of the response system

However, the NDB scheme has not fully resolved the problems it seeks to address, and the current application of the scheme warrants review. The primary shortcoming of the scheme is the way in which it frames the obligations and incentives of different actors within the data breach response environment. Because the obligations of the NDB scheme end at notification – that is, because organisations have fulfilled their legal duties under Part IIIC once they have notified impacted individuals – there is little incentive to take additional measures that are beneficial (and often necessary) for the consumer.

Consequently, the NDB scheme has resulted in organisation-centred approaches, where the emphasis is on assessing the breach and notifying the regulator and individuals, without necessarily considering the more substantive objective of consumer protection. In short, organisations' efforts end where their legal obligations and incentives end.

There are some exceptions to this. Organisations with a better understanding of the response environment and individuals' needs do more than just notify. They provide practical advice to individuals and offer various services to assist – for example, employers that have experienced a data breach involving the personal information of employees may give the employees paid time off to address the risks. Organisations may also provide credit monitoring services for individuals, reimburse them for the cost of replacing compromised credentials, provide a dedicated communication channel to answer any queries, refer individuals to specialist support services such as IDCARE, and in some instances, contact relevant organisations on behalf of impacted individuals, such as credit reporting agencies and relevant government agencies, to inform them of the data breach.[15]

This approach, however, is not common practice. In most instances, primary responsibility falls upon the individual whose personal information has been compromised. Notification is simply the beginning of a much longer process The individual is responsible for communicating with relevant organisations to protect their personal information from misuse. This may include contact with credit reporting agencies, financial institutions, telecommunications companies, law enforcement, government departments such as the Australian Taxation Office and the Department of Human Services and transport departments, and any other organisations with which the individuals holds accounts.[16]

There is very little communication between entities; most communication proceeds through the individual. This is despite the fact that the individual was not responsible for the data breach, and many of the steps taken post-notification are for the benefit of the organisations; if identity fraud occurs, the financial loss will typically be carried by the organisation that provided the goods or services in question.[17]

[15] IDCARE, *Beyond the Breach: How Post-Notification has become the Real Race* (July 2020) 5-6.
[16] Megan Wyre, David Lacey and Kathie Allan, 'The Identity Theft Response System' (Trends & Issues in Crime and Criminal Justice No 592, Australian Institute of Criminology, March 2020) 9-12 <https://www.aic.gov.au/publications/tandi/tandi592>.
[17] Ibid 9.

Moreover, given the immaturity of the response system and the emphasis on the individual to complete tasks, proceeding through the response systems often causes harm for individuals. The time and stress involved in navigating the response system is exacerbated when individuals receive a notification that does not identify the types of personal information compromised or provide accurate advice on the steps an individual should take.[18] Individuals may also receive incorrect or contradictory advice from organisations as they proceed through the response system.

The current system needs to be improved. The law should not define notification as an end in itself; it should be considered a means to end. The objective should be to assist individuals to protect themselves from the misuse of their personal information. Individuals can be assisted by improving the maturity of the response system – for example, by developing a multi-institutional, coordinated response to data breaches.[19] There needs to be greater capacity and willingness for organisations to undertake tasks on behalf of impacted individuals and to communicate with each other. This solution may require legislative action – for example, some overseas jurisdictions require organisations to not only assess whether misuse is likely to occur, but whether misuse *has* occurred and, in some circumstances, to notify credit reporting agencies following a data breach.[20]

2.2. Threshold for notification

The operation of the NDB scheme could also be improved by amending or clarifying the threshold for notification. APP entities are required to notify the OAIC and impacted individuals when a data breach is "likely to result in serious harm." Serious harm is not defined in the legislation and there is no delineation between serious harm and non-serious harm. While the NDB scheme was introduced primarily to

[18] IDCARE (n 15) 4.
[19] Paul M Schwartz and Edward J Janger, 'Notification of Data Security Breaches' (2007) 105(5) *Michigan Law Review* 913, 918, 960.
[20] See for example, Kan Stat Ann §§ 50-7a01–7a04 (2019). For a more general discussion, see Dana J Lesemann, 'Once More unto the Breach: An Analysis of Legal, Technological, and Policy Issues Involving Data Breach Notification Statutes' (2010) 4(2) *Akron Intellectual Property Journal* 203, 215; Jacqueline May Tom, 'A Simple Compromise: The Need for a Federal Data Breach Notification Law' (2010) 84(4) *St. John's Law Review*, 1569, 1583-85.

address the risk of identity theft, it is clear that other forms of harm are encapsulated under "serious harm", including physical, psychological, emotional, financial and emotional harm.[21] The legislation provides several factors to consider in assessing the risk of harm,[22] but it is unclear how these factors are to be weighed or how to draw a distinction between serious and non-serious harm.

2.3. Definition of "personal information"

The NDB scheme also incorporates the same broad definition of "personal information" used throughout the Act, which includes any information or opinion about an identified individual, or an individual who is reasonably identifiable.[23] The ALRC recommended adopting a substantially narrower definition of "personal information" for the NDB scheme,[24] and it is common in other jurisdictions to use a definition of personal information that reflect the types and combinations of personal information that are more likely to present a serious risk to individuals (for example, an individual's driver license number, account number or credit or debit card number, health information or biometric data).[25] The current definition means that unauthorised access to or disclosure of *any* type or combination personal information may require an organisation to assess the breach and to determine whether notification is necessary by reference to a threshold ("serious harm") that is not defined.

2.4. Two-tiered notification

If, despite these deficiencies, there is reluctance to amend the current scope of the NDB scheme, the legislation could set a lower threshold for notifying the regulator before requiring notification to impacted individuals. This would enable

---

[21] Explanatory Memorandum, *Privacy Amendment (Notifiable Data Breaches) Bill 2016* (Cth) EM 3 [9], 72-73 [41]-[42]; Office of the Australian Information Commissioner, *Data Breach Preparedness and Response: A Guide to Managing Data Breaches in Accordance with the* Privacy Act 1988 *(Cth)* (July 2019) 33.
[22] *Privacy Act*, s 26WG(c)-(j).
[23] Ibid s 6.
[24] Burden, Lane and Nessen (n 8) 303.
[25] See for example, Cal Civ Code §§ 1798.29, 1798.82.

organisations that were unsure of the risk of harm to consult with the OAIC and prevent unnecessary notification for individuals. The OAIC would benefit from a more complete view of the data breach and cyber security landscape, and would be able to use that broader understanding to guide organisations on how to notify and what advice to include in a notification.[26]

The European Union's *General Data Protection Regulation* provides an example of two-tiered notification. Regulated entities are required to notify the regulator of a data breach unless the breach is unlikely to result in a risk to the individual's rights and freedoms.[27] Entities are required to notify impacted individuals unless the breach is unlikely to result in a *high* risk to the individuals' rights and freedoms.[28] Where an entity notifies the regulator, but has decided notification to individuals is not required, the regulator can require the entity to notify individuals if it believes the threshold has been reached.[29] This provides for greater involvement on the part of the regulator. It enables the regulator to bring its expertise and experience to bear, while also providing some reassurance for entities.[30]

[26] Schwartz and Janger (n 19) 966-68.
[27] *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)* [2016] OJ L 119/1, art 33.
[28] Ibid art 34.
[29] Ibid art 34(4).
[30] Bernold Nieuwesteeg and Michael Faure, 'An Analysis of the Effectiveness of the EU Data Breach Notification Obligation' (2018) 34(6) *Computer Law & Security Review* 1232, 1244.