Privacy's Balancing Act

Are we expecting too much of a reasonable person?

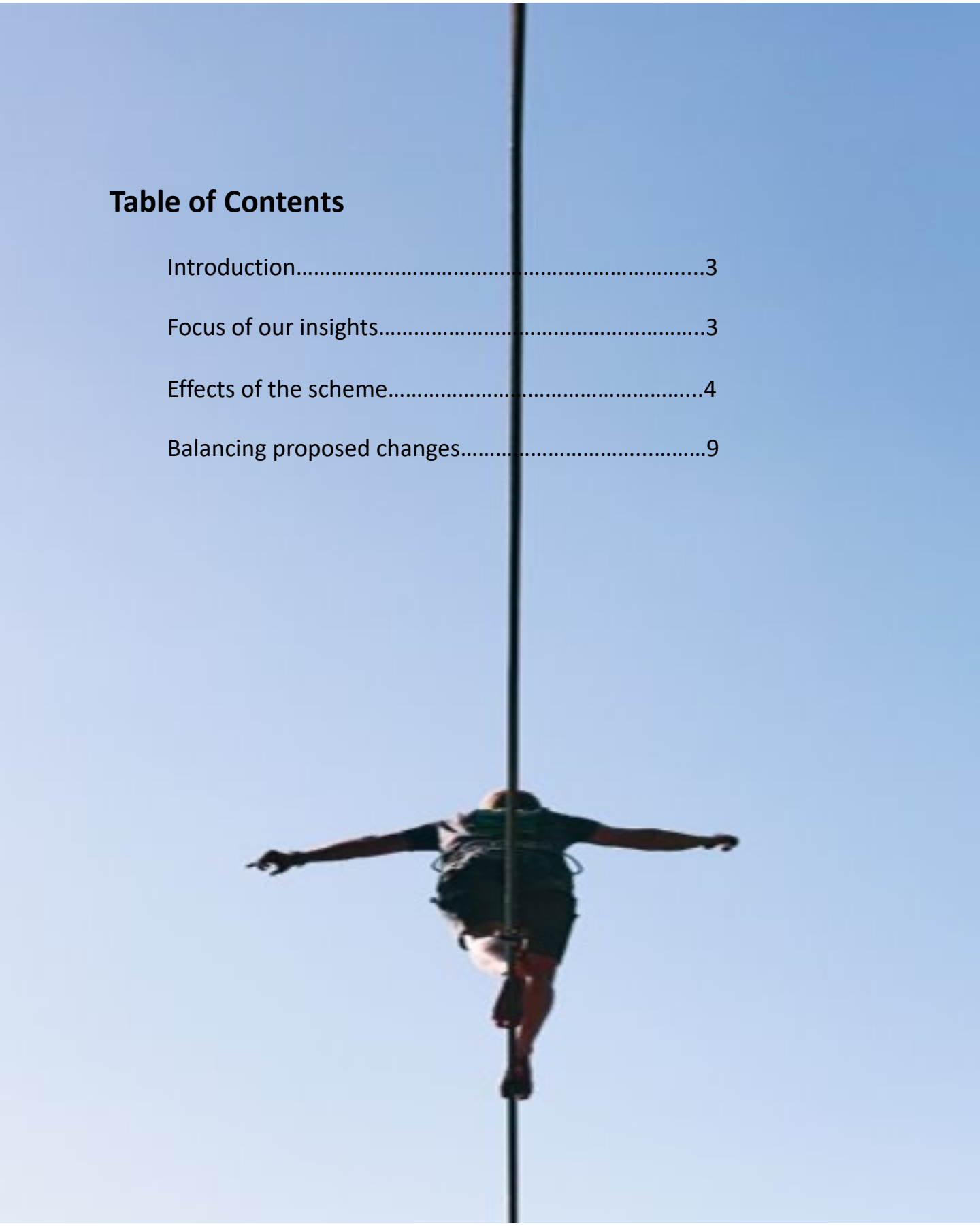


Table of Contents

Introduction

1. We may have a legal right to privacy, but increasingly for consumers, not a practical right. It is impractical to read for 40 minutes a legalese privacy policy whilst standing in a busy queue, and then make a decision to forgo personal information in order to access an essential service just to appease the authors of such policies that consent (and compliance) have been blissfully achieved. Consent has been a hallmark of privacy regimes for many years, but there is little doubt we are up against it in terms of fighting its impracticalities.

2. What's relevant to this report and the insights IDCARE can offer are the recent additions to privacy regimes in relation to notifiable breaches. Relevant because IDCARE has spoken directly to many tens of thousands of people about notifications they have received and the impacts to them to flow from the breach of their data and efforts to remediate risk. We've been a witness and bystander to the mechanics of many successful and not so successful incident response teams and watched, sometimes with amazement, how stakeholders have attempted to shape and influence a breach outcome. These perspectives are further informed from the ongoing monitoring of groups responsible for many of the most abhorrent breaches and the criminal vendors who prey upon breached data for profiteering purposes we carry out in order to proactively find and inform impacted persons, organisations and regulators.

3. None of these insights would be useful without persistent testing of our response system and its affordances for people who are breached. The testing is not aspirational based (i.e. how an organisation or government hopes to assist impacted persons), but the lived experience and reality from both community members who have engaged organisations and our own testing of such entities. All of this is done independent of government and business, driven by a purely charitable aim of mitigating harm to impacted communities from these events. It is a perspective that is extremely unique and one we hope will have a unifying voice for the many interests that invariably vocalise when it comes to much needed privacy debates.

Focus of our insights

4. Since 2018 in Australia and 2020 in New Zealand, entities falling within these privacy regimes have a legislated requirement to notify the regulator and the impacted person where there is a reasonable belief that the breach has caused or is likely to cause someone serious harm. The test of serious harm is inevitably a conflicted one. It is the breached entity or their appointed advisors that come to this view. It includes governments seeking to protect their programs from exploitation and abuse. Lost in amongst the crisis-inspired jockeying are often the impacted persons. It seems the orientation of our frameworks when it comes to eligible breach events are less about informing and supporting a person to take-action who has been placed in a potentially vulnerable position, but more about a need for 'tick a box' reporting to regulators and to protect other interests. Conflicts within this environment are aplenty and the proposed reforms in Australia are likely to take these conflicts to a higher level.

5. This report captures these tensions in the context of key elements of the Privacy Act Review. It highlights where there are opportunities to rebalance and achieve common needs of both the individual, the organisation and the broader market. Whilst it is a natural proposition for any government to consider increasing penalties, it's probably not the first order issue in terms of finding more meaningful outcomes that return us to the overall intent and purpose of any privacy regime – our fundamental right to privacy and its protection.

6. There are two thematic elements to this report. First, is a reflection on the key elements of the existing legislation's broader context and intent. Specifically, this report reflects on the Act's Explanatory Memorandum relating to the 2018 amendments that introduced the notifiable data breach scheme in Australia. Foundationally, this is important, as it enables exploration of IDCARE's observations and how these have empirically changed (or not) since 2018. This sets the scene for contributed thoughts and analysis relevant to our work that can inform the current Privacy Act Review (2022) commissioned by the Commonwealth in seeking to modernise the Act.

Effects of the Scheme

7. Legal remedies beyond complaints to the regulator in alleged non-compliance with privacy laws are set to increase, as recently seen in efforts to bring about class actions (albeit tangentially in their focus on consumer rights and corporate and market responsibilities). It's important to reflect on the ways in which courts may interpret our privacy laws. The modern approach to statutory interpretation is best articulated by Justice Spigelman in that 'the law is a fashion industry. Over the last two or three decades the fashion in interpretation has changed from textualism to contextualism'.[1] Putting it another way, the judiciary when contemplating specific statutory provisions where the text may provide alternative conclusions, literal interpretations of words may need further contextualisation in both materials within an Act (intrinsic materials), and extrinsic materials. One accepted source of extrinsic material is a Bill's explanatory memorandum. This provides our analysis with a useful reference point in unpacking what the actual purpose and intent of our privacy laws hold.

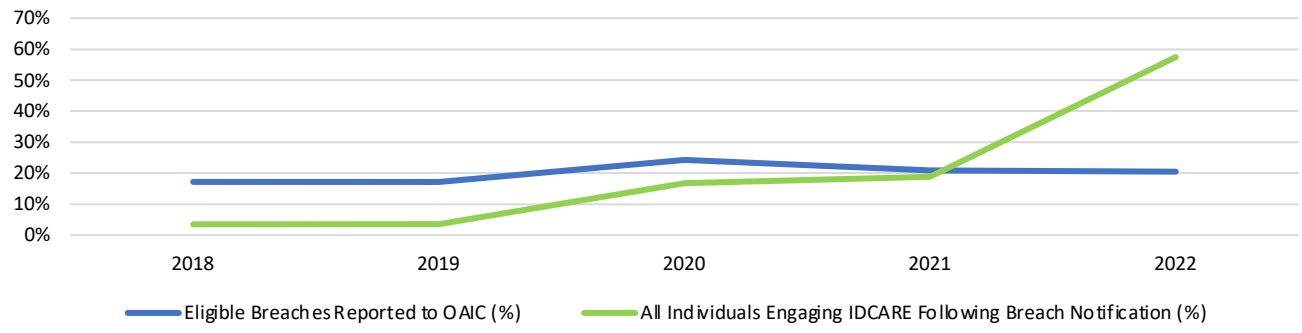
8. What mischief presents that would otherwise be left unchecked if amendments were not passed? The chance to remediate against risks of serious harm is a clear one in this context. For the purposes of the elements of the *Privacy Act 1988* (Cth) that relate to the notifiable data breach scheme the explanatory memorandum of relevance to this reflection is the *Privacy Amendment (Notifiable Data Breaches) Bill 2016 Explanatory Memorandum*. It provides that the objective of the *Privacy Act 1988* (Cth) is to 'promote the protection of privacy of individuals, while recognising that this protection should be balanced with the interests of entities carrying out their legitimate functions or activities'.[2] This legislation by definition is a **balancing act** between the privacy interests of individuals and the privacy infringing acts of regulated entities required to deliver their business (or government) purpose.

9. IDCARE is best left to comment on those elements of the *Explanatory Memorandum* that rely upon our insights and observations as part of the current legislation's suite of interpretive sources. This then sets up our analysis of the relevant Privacy Act Review proposed amendments by commenting on intervening changes to the context and the related mischiefs these seek to address.

The mischief of identity theft and its remediation

10. A strong theme as a basis for a notifiable breach regime is on the risk of identity theft and other serious harms and the need to create opportunities for individual remediation. IDCARE's demand from the community since February 2018, the commencement period of the data breach notification scheme, has grown by 358%. For community members impacted by data breaches this has increased by more than 1,600% over the same period. The below graph visualises this growth since the Australian amendments in 2018 compared against the reports of eligible breaches to the regulator. The dramatic divergence is driven by individual events resulting in much higher numbers of exposed persons.

Eligible Breaches Reported to OAIC[3] and Breached Community Member Engagement with IDCARE
(% of Accumulated Total from 1 April 2018 to 31 December 2022)



[1] James J Spigelman, 'From Text to Context: Contemporary Contractual Interpretation' (Speech, Risky Business Conference, Sydney, 21 March 2007) 1.
[2] Commonwealth of Australia, *Privacy Amendment (Notifiable Data Breaches) Bill 2016 Explanatory Memorandum*, 2016 [112].
[3] Office of the Australian Information Commissioner (2018-2023) Notifiable Data Breaches Reports accessible via the following search string: https://www.oaic.gov.au/search?query=Notifiable+Data+Breaches+Report&sort=dmetapublishedDateISO&num_ranks= (Accessed on 23 March 2023)

The mischief of identity theft and its remediation (cont.)

11. It's certainly evident that more people are aware that their information has been breached and are actively seeking ways to mitigate the risks of serious harm that follow such breaches. We do not see any evidence of 'notification fatigue' by impacted persons during this period; in fact we see the opposite. The largescale breaches reported in September and October 2022, did heavily influence volumes of community engagements to IDCARE's specialist services. Web content relating to IDCARE's specialist advice to impacted persons received over a million views during the last quarter of 2022 alone as a further indicator of active interest in remediating by notified persons. Now our focus is drawn to supporting community members that have to deal with aggregate risks resulting from multiple proximate breach events.

12. Whilst we see no evidence of 'notification fatigue', we are seeing a growing level of anger and discontent about remediation. This is particularly directed by community members in relation to remediating government-issued credentials every time they are exposed. The scale of some incidents and their amplification by the media generated countless media statements that projected complex advice and views that were factually wrong and misleading to the public and people directly impacted. This is a highly complex issue and one that does not at present lend itself to any adequate and reasonable solutions for impacted persons or safeguards in the actions taken. More on this topic is covered in the latter part of this report.

13. A clear purpose of the notifiable data breach scheme is to allow impacted people to take remedial action. Interestingly, when we examine notified breaches over the last twelve months, the actual numbers of persons to present to IDCARE in the belief that their breached personal information had resulted in identity theft or fraud was only a very small fraction of notified persons (around 0.8%). Over the four year period since the amendments were passed, the average misuse rate was 6.7% for notified persons. This doesn't of course mean that everyone else was immune from post-breach exploitation, but it does illuminate in broad terms particular elements of the risk environment. What would a *reasonable person* say if they were told that between 93.3% and 99.2% of people to be notified of a breach wouldn't experience identity theft and related serious harms to necessitate specialist support? What would their expectations be of remediation and response? Perhaps this doesn't matter, as it's clear the regime only requires that the likely risk of serious harm present to only one of the breached individuals (i.e. 'someone'). That we can almost be assured will occur. We can also be assured, being upset or distressed about a breach notification and event is not likely to reach the lofty heights of seriousness. Of course the circumstances may mean that our *reasonable person* may not always agree, such as when a person's physical address is included in the breached attributes and such a person is a participant in a witness protection program or is a survivor of stalking or other abusive context. Clearly risks, actual or perceived, elevate in these scenarios.

14. But how would the *reasonable person* (the breached organisation) even know that this is a risk in a particular circumstance? More often than not, they wouldn't, and in IDCARE's observations of incident responders across government and business, judgments tend to be made on this specific issue based on the size of the breached cohort (i.e. the larger the numbers of persons breached, the more likely incident responders will assess that a person will be impacted adversely in this way). We've seen some areas of governments lean on access to other government data repositories to assist in identifying cohorts that may be living in such environments as part of their assessment of such risks. But this too is fraught practice. Government repositories provide no absolutes, can be out of date (or not timely enough) and incomplete. Is such probing alone by other parts of government that could be completely unrelated to the context a breach in its own right? These are the many practical conundrums confronting incident response teams. Placating these realities by proclaiming that a regulator *should* or *may* develop guidelines or standards is arguably insufficient in this context. Alternatives to this are presented later.

Criminal market exploitation of breached data

15. Another reason for the vast majority not reporting serious identity exploitation harm following a breach, may be that there is so much personal information that has been exposed and is in circulation, such as via darknet markets, that the chances of being the individual actually targeted by identity thieves is remote. During 2022, IDCARE identified 183 unique listings of Australian driver licence scans on darknet forums and those sold online outside of the darknet. Some of these listings were promoting an unlimited supply of credentials. The average cost of these scans across darknet markets is $75 AUD, although, they can sell for as little as $1.50 AUD. In 2022, the average price of an Australian passport scan sat at around $52 AUD. These prices represent a continued decline in the market value of breached credentials, indicating that criminals have an oversupply of credential exploitation options or indeed have found alternative means to achieve their criminal enterprise.

Darknet posting from ransomware group in February 2022

16. In January 2023, IDCARE monitoring of online environments specialising in the extortion of breached entities and the recirculation of breached data revealed that Australia was ranked fifth in terms of the most targeted nations by such groups. A significant reason why Australian governments and businesses are increasingly targeted by ransomware attacks, the likes of which have breached almost half the Australian population in the last twenty-four months, is because we pay. Business is booming for ransomware attackers because there is little disincentive and Australia has form in paying and not necessarily notifying. In a recent report by forensic accounting firm McGrath Nicol (2022)[4], a survey of 500 Australian business leaders on their experiences with ransomware found that:

- 59% of businesses surveyed experienced a ransomware attack in the last five years;
- 79% of businesses chose to pay the ransom;
- 44% would pay a ransom within 24 hours to minimise the potential damage; and
- The average ransom paid in 2021 was $1.01m AUD.

17. Put simply, in terms of ransomware attacks, Australia is open for business. There is little acknowledgement of this fast-growing threat in the *Privacy Act Reivew* but it is front and centre the main driver for the largest breaches confronting our community and almost certain to confront our community going forward. When coupled with some cyber insurance firms calling out that their cover may include the payment of ransoms, and little to no enduring enforcement intervention, there is little disincentive for these criminals to keep targeting Australian businesses and government agencies. This is further exacerbated by the conflicting nature of compliance and notification environment. Pay a million dollars or face a breach that may cost $50 million. Pay a million dollars or face a third of your customer base leaving. Don't pay and have your customer data exploited in the most abhorrent and public way in an attempt to send a clear signal to future organisations that this will be the consequence if their demands are not met. The weaponisation of personal information is real and the refining of ransom demand practices continue to maximise criminal opportunities. The conflicting nature of breach response and regulatory compliance, coupled with an insurance industry that in some places openly promotes their coverage of such payments, presents a perfect storm for our community and our ability to protect against these privacy infringements.

18. An obvious strategy may be to advance from the policy statement that 'government does not endorse the payment of ransom' to one that creates a specific offence category for ransom payment.

[4] McGrath Nicol, 'Ransomware on the rise' (2022). Located at https://www.mcgrathnicol.com/app/uploads/McGrathNicol_Flyer-Ransomware-on-the-rise_Final.pdf

Criminal market exploitation of breached data (cont.)

But there are many complexities to this. Arguments against a more heavy-handed approach to ransom payment being an offence category narrows quickly to one of business continuity, and in some cases, survivability. One Sunshine Coast business IDCARE supported in their ransomware attack had no means of recovering customer and employee files. They couldn't process orders and they had no quick way of meeting payroll obligations. Their insurer pushed them to a specific law firm and a cyber forensics provider that quoted around $15,000 a day to assist due to policy coverage shortfalls. The ransom payment was less than the amount they were looking at paying to remediate per day. There was no technical assistance available from government and no prospect that the criminals responsible would be brought to account. In our estimation, the drawing into the Privacy Act of small business is likely to see these scenarios amplify.

19. IDCARE is not convinced that the absence of reporting and notifications are solely driven by these dire circumstances. We know there is a conceivable absence due to the volume of community members coming to IDCARE unaware of how criminals first got hold of their personal information that is being exploited. In other words, we believe that organisations are making decisions to not notify because they or their legal advisors believe that the payment of a ransom remediates the risk. Sadly, we don't see this reality. The number of community members engaging IDCARE who do not know how their personal information has been breached has remained relatively steady at 18% since the introduction of the notifiable breach laws in 2018. The fact that almost one in five people don't know the source of their breached information may be partly explained from failed attempts by organisations to notify the individuals. This statistic is closely held by breached organisations, but in some matters IDCARE has seen this as high as one in three.

Perverse outcomes from increasing penalties

In the absence of regulatory intervention that prohibits or provides disincentives for a ransom payment, or at least places extreme limitations on when it may be contemplated (such as a significant going concern risk), it is unlikely ransomware groups targeting our organisations will curtail their activities. Legislative changes to increase privacy act penalties may actually have a perverse result, such as reducing future reporting of such attacks, because of the conflicted environments many confront. Some law firms over the years have advised payment as a means to lean on the remediation exemption – that is, the criminal has said they have destroyed all copies and haven't shared, therefore the breach is contained and there is no serious risk of harm. Leaning on the *reasonable person*, if they had the full circumstances, they would likely see what IDCARE sees and that is the re-emergence of data from previously met ransom demands. This alone gives little material effect to the hacker subsequently withdrawing the demand and stating that they have destroyed the only copy of the data. The reality is that data remains accessible even today. It is foolish to believe the payment of a ransom leads to the data being deleted and not shared. To lean on this as an exemption to notify is a legal furphy. Over the last twelve months, IDCARE witnessed a change in a number of offerings on the darknet to advance the exploitation of breached data. Among these were vendors offering data aggregation services where breached organisational data, including those that were subject to a ransom payment, were offered for sale as 'mega breached person packages'. This counters the argument that paying a ransom actually lessens the risk of sharing and subsequent exploitation. An absence of this direct issue being addressed in the Privacy Act Review is a significant shortfall in the reform agenda. It may in fact be a symptom of bureaucratic organisation, where cyber, privacy and corporate regulation diverge into Ministerial responsibilities, but it is a key gap.

General awareness about exposed personal information

20. The Office of the Australian Information Commissioner (OAIC) under the voluntary reporting regime received on average 70 breach reports per annum from 2009-2010 to 2015-2016, compared to an average of 871 breached entity reports per year under the notifiable regime introduced from February 2018.[5] At a fundamental level, certainly the 2018 amendments have driven higher levels of awareness about the exposure of personal information that could lead to serious harm. This would contribute directly to a key legislative amendment purpose in first establishing the scheme to enable notified persons to remediate such risks.

Time as an important factor to consider

21. The prior amendments to the Privacy Act also referenced in their explanatory memorandum the element of time. That is, the time taken to notify impacted persons and the time between compromise or breach and recorded exploitation. Since 2018, the average time taken to detect the exploitation of personal information captured by IDCARE community engagements has been 32.7 days. The time between a breach and the identity theft exploitation of the breach where detected was 16.3 days. These timings have altered dramatically when compared to the breach landscape prior to the notifiable data breach scheme's introduction from IDCARE's community engagements. Insights captured from community members during 2015 and 2016 reported that the average time between a breach occurring and an individual being notified (voluntarily) of a breach was 405 days. The time between breach and misuse was 72 hours. These are dramatic changes in our understanding of critical time metrics. On a positive note, the significant reduction in the time taken to notify can only be seen as welcoming for impacted people.

[5] Office of the Australian Information Commissioner (2018-2023) Notifiable Data Breaches Reports accessible via the following search string: https://www.oaic.gov.au/search?query=Notifiable+Data+Breaches+Report&sort=dmetapublishedDateISO&num_ranks= (Accessed on 23 March 2023)

Balancing proposed changes

22. The proposed amendments are almost certainly going to result in four clear outcomes if implemented. The first is that privacy compliance will become much more litigious in Australia. We are already seeing actions initiated on the grounds of consumer law compliance, corporate law and market regulation. If amended as proposed, we will invariably see an advancement of a privacy tort and court remedies for impacted persons. One positive outcome is the common law, at least when it comes to notifiable breach compliance, will advance and continue to mature. At present there are few cases that deal with the specific legislative provisions, particularly in relation to notifiable breaches, serious harm, and what a reasonable person may expect in relation to remediation. The judiciary landing on their interpretation of these tests and arguably subjective terms may in some quarters be welcomed.

23. The second certainty, and most obvious one, is that we will continue to see large-scale breaches. It is a certainty that these will increase in severity and volume as the proposed amendments are likely to do little to curtail these events. This is a case of what's not in the proposed changes. The devasting impacts of ransomware attacks on the community without regulatory intervention, including appropriate resourcing for the regulators, and market levers to create disincentives to pay and incentives to prevent, will continue to drive these criminal behaviours.

24. Increasing penalties for privacy non-compliance may well have a perverse outcome to push such events even further underground. IDCARE is likely to see even greater numbers of community members fall within the "unknown" compromise category. The conflicted nature of breach assessments and notifications will largely influence such practices.

25. Finally, we will also likely see continued remediation challenges. Of late the trend has been for governments to influence the provisioning of the actual breached data under the auspices of protecting government programs. In other words, breached entities are being requested to provide government with the breached data. The practical consequence of this has been that breached individuals are having to remediate via the replacement of credentials because the breached credential information is being flagged on national systems as being invalid. Whilst there is merit in these steps, without consent by the impacted person, there are considerable risks that the actual notification by the breached entity which may either inform the person that these measures have been taken on their behalf (or in many cases not), either does not reach the breached person or the consequences of doing so are not that well articulated. The messiness of this response system for the actual impacted person is problematic. Complaints from community members being denied access to products and services because remedial action has been taken without their consent through these measures are increasing. A non-consent based approach appears to be contrary to a key tenant of our privacy laws – that is, impacted people are notified and *they* have the opportunity to take remedial action. When this is done on their behalf without their awareness, and then transpires into other harms, such as being denied a mortgage or personal loan because their identity credential is determined to be invalid. These acts of remediation in and of themselves is likely to cause the actual serious harm. This is further exacerbated when the actual rate of identity exploitation and misuse in breach events is extremely low.

26. These scenarios will become increasingly messy. Since September 2022, more than 30 million records relating to personal information have been breached across just four breaches. Some community members have been impacted by all of these. The practices mentioned in terms of proactive protection necessitates that the individual impacted may need to replace their credential four times in six months. Whilst this may create a useful stream of revenue for credential issuers in continually having to support credential replacement, it seems more a band aid solution to a much more fundamental issue around our identity system.

Balancing the proposed Act amendments (cont.)

27. The more likely scenario with these practices is that for many they won't know that their credential is invalid until they seek to use it in applying for new products or services with completely unrelated parties to the data breach. They will be denied these services and some will think that their identity has been stolen or some other criminal mischief has occurred – as we are already seeing unfold. What does this even mean for prior breaches? For example, those breaches that up until September 2022 involved driver licence exposures where the ability to replace their old licence with a new driver licence and card number wasn't extended as a remediation strategy. Are people who have been historically breached and notified about such breaches going to be re-engaged because the response system affordances have now changed and there are protective measures in place today that weren't when they were first notified? As a policy position it may be that the thinking here relates to the eventuality that these credentials will expire in any case, and that the same outcomes will eventually be realized. But for some, that may not be for another five to ten years. Reverting back to one of the key pillars of our privacy regime, shouldn't the individual have that informed choice to make?

28. These points highlight the need for consideration of a formal structure involving representatives from industry and government in the ongoing design of standards of practice and directives (advice) in relation to notifiable breach responses. By this we do not mean only drafting and allowing comment and input on such drafts originated by government. The testing IDCARE performs on the response system is critical to our understanding of response system affordances. Coupled with direct community engagement, the knowledge we accumulate is vital in shaping the best possible outcome for impacted persons. However, governments and businesses acting unilaterally without this collective view is very risky, and what we are witnessing transpire in terms of serious harms presenting from the actual remediation measures taken by these organisations are a case in point. There are models that exist in other contexts where joint bodies can be formed that assist to make not just codes of practice and guidance, but practical directions and authorities requiring short turnarounds (in this context as breaches are unfolding). The nature of the data breach landscape calls for agility, specificity, and an intimate understanding of the consequences of decisions that for some will impact millions of Australians. IDCARE's work is deliberately independent of government. We are free to provide the advice we see as critical to the impacted person. This advice is free from what a commercial entity or government agency believes is in their specific interests. That's a big reason why this independence is so important and why the community entrusts IDCARE to provide that independent and impartial advice. Our challenge is one of accessibility and functional design. Related to this is a sense of how IDCARE can feed a collective and contemporary view of risk of harm and response affordances designed in a manner that gives the individual choice. We do not see the proposed amendments recognising this requirement. It does not acknowledge the real remediation challenges and the lack of market knowledge of an evolving risk and response environment. Thinking that remediation, as articulated in the 2018 *Explanatory Memorandum,* can simply mean 'changing passwords' belittles the real complexities of our response system.

29. Other proposed amendments to the Privacy Act will no doubt require further details. The right to access, whilst already established, in the context of our work would benefit from clearer guidance on the ability for organisations, like IDCARE, to act on behalf of vulnerable community members. Too often community members lament at denials to access the information about them criminals have used to exploit their personal information. IDCARE finds similar responses where we seek to act on behalf of vulnerable persons. The 30 day timeframe for such requests is severely inadequate for individuals who are experiencing identity exploitation unfold before their very eyes. There must be contemplation of a different standard for victims of identity exploitation that dramatically narrows response timeframes and removes costs associated with such access.

Balancing the proposed Act amendments (cont.)

30. Rights associated with erasure is an interesting concept. If these amendments are made, regulated entities should expect that almost every community member engaging IDCARE would request this action across multiple entities. This would likely result in more than a million requests from identity theft and misuse victims per year, let alone those you would reasonably expect would want the same outcome from an entity responsible for a data breach. Like a number of provisions proposed, detail is necessarily needed to be fleshed out on the practical realities of such changes when their form and structure is further developed as proposed amendments. We would expect a similar consequence would present in the de-indexing environment.

Conclusion

31. There are many changes proposed that require much deeper analysis and consideration than the time allowed to comment. We have provided within commentary and perspectives we feel IDCARE is best placed to reflect upon in the hope that it does inspire discussion and debate. We have much to gain from modernising the Privacy Act, but many lessons to learn from even the changes applied since 2018.

March 2023