Privacy Act Review Report consultation

PwC Submission
March 2023

pwc

Via AGD submission portal

31 March 2023

Consultation into the Privacy Act Review Report and Proposals

To whom it may concern,

PwC Australia welcomes the opportunity to provide this submission to the Attorney-General Department's consultation into the *Privacy Act Review Report* and its proposals. We commend the Federal Government for its commitment to ensuring the *Privacy Act (1988) (Cth)* (the Act) remains fit-for-purpose in a digital age, in which threats to privacy are increasingly complex and varied.

Given the breadth of our work and the diverse clients we work with, PwC has unique insights into the opportunities and challenges the reform process presents, which are included within this submission. We trust this contribution will support the government's overall goal of ensuring these important reforms provide tangible benefits to Australians, while being carefully balanced with the regulatory burden being placed on affected organisations.

Furthermore, this process presents a unique opportunity to harmonise the patchwork of divergent privacy-related laws and regulatory frameworks that currently exist at federal, state and territory levels, as well as globally, creating a more streamlined regime with reduced duplication. Ultimately, harmonisation will help individuals better understand their privacy rights and reduce the regulatory burden for organisations that have privacy-related obligations under multiple regimes.

For ease of reference, our submission contains a detailed Executive Summary and high-level overview of Our Key Submissions. Detailed responses to relevant proposals are drawn out further in Our Response to the Proposed Privacy Reforms.

Again, thank you for the opportunity to contribute to this important consultation. If you have any queries or would like to discuss this submission further, please do not hesitate to contact either of us on the phone numbers or email addresses below.

Yours sincerely,

Jon Benson
PwC Australia Partner
jon.benson@pwc.com
0438 565 299

Adrian Chotar
PwC Australia Partner
adrian.chotar@au.pwc.com
0457 808 068

Contents

Executive summary

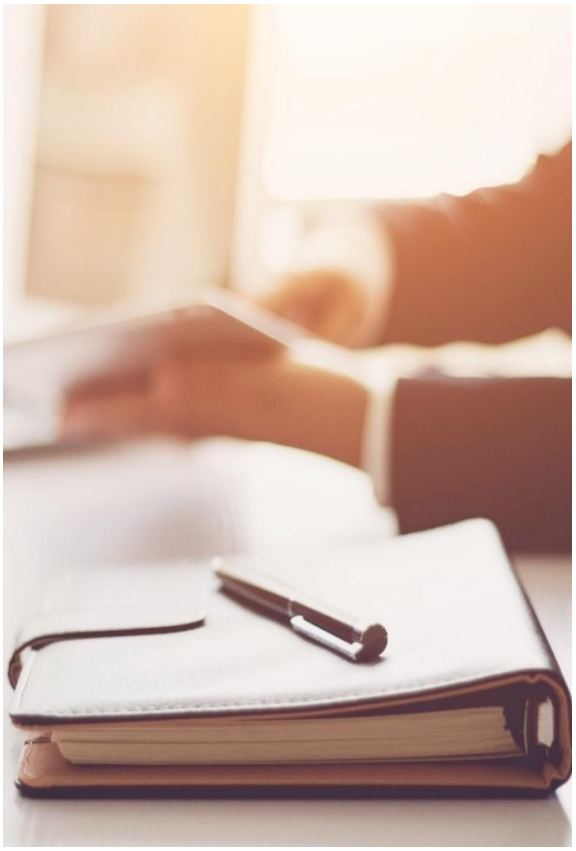
In a rapidly evolving digitised world, in which the day-to-day services, systems and processes Australians rely upon are increasingly delivered via connected platforms, there is an urgent need to ensure our nation's privacy laws are fit-for-purpose and future ready. There is clear evidence Australians are increasingly concerned with the protection of their personal information (PI), especially in the digital domain, with the most recent figures from the Office of the Australian Information Commissioner (OAIC) indicating 87% of Australians want more control and choice over the collection and use of their PI.[1] And, as noted in the OAIC's most recent six-month report (July to December 2022), Australia experienced a 67% increase in large-scale data breaches.[2] Therefore, doing nothing is not an option.

While protecting the privacy of Australians is vitally important and reforms to the Privacy Act 1988 (Cth) (the Act) are necessary, the process must take into account the regulatory burden this could present for captured organisations. For many, substantial technology and operational uplift will be required for compliance, which ultimately comes at a cost to these organisations and, in turn, consumers. Studies have shown that the introduction of GDPR did come at a cost, with profits shrinking by an average of 8.1 percent in 2018 after GDPR's introduction, with a greater burden falling on small to medium businesses.[3] Therefore, helping organisations bear the brunt of additional regulatory and cost imposts the reform process could entail should be considered.

Australia is at risk of falling behind globally if positive progress is not made, putting at risk our ability to effectively interact in the global digital economy. As noted by the OECD, "the effective use of data can help boost productivity and improve or foster new products, processes, organisational methods and markets. Although there is still little reliable quantification of the economic effects of data use, firm-level studies suggest that firms that use data exhibit faster productivity growth than those that do not, by approximately 5% to 10%".[4] Further, the failure to undertake effective privacy reform could jeopardise Australia's aspirations to become a leading digital economy over the next decade.

To alleviate compliance burden for organisations* and to create a more streamlined set of directions for Australian organisations, we submit that a cornerstone of this reform process should be a focus on better harmonisation of Australia's PI-related regimes supported by a **clear and prescriptive** approach. There is a current patchwork of privacy-related obligations across multiple legislative and regulatory regimes, with significant duplication. This opportunity to create a holistic and integrated regulatory framework must also consider consultations and inquiries currently underway, such as the 2023-30 Australian Cyber Security Strategy Discussion Paper (which raises the prospect of expanding the Security of Critical Infrastructure Act (2018) (SOCI) to capture 'data'), and the Digital Platform Services Inquiry - September 2022 Interim Report (which touches on privacy-related aspects of digital platforms operating in Australia[5]).

For ease of expression, the terms 'organisation' and 'APP entities' are used interchangeably throughout this submission.



[1] https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2020-infographic
[2] Notifiable Data Breaches Report: July to December 2022 | OAIC
[3] Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally
[4] Interoperability of privacy and data protection frameworks | Going Digital Toolkit Note, P 11
[5] Digital platform services inquiry - September 2022 interim report - Regulatory reform | ACCC

This submission aims to strike a balance between the need to reform the Act and the potential impacts and consequences for regulated organisations. We have also submitted ideas as to how these complexities could be addressed to ensure an appropriate scope of reform is achieved.

To this end, three key themes run through this submission:

1. **The opportunity for trust and value - both commercial and operational - these changes present for Australian organisations and the broader community.**
2. **The opportunity this process presents for harmonisation of privacy-related laws and regulations.**
3. **The practical challenges and potential burdens that organisations may face as a result of these reforms, and the importance of leadership.**

The opportunity for trust and value - both commercial and operational - these reforms present for the Australian organisations and the broader community

If we get this right, individuals will have greater confidence and be empowered to participate in the digital economy. Australians have been fast to embrace digital technologies - in the immediate response to COVID-19, it is estimated the community has vaulted forward five years in consumer and business digital adoption.[6] However, for the digital economy to operate optimally, trust and data protection are integral, with recent data breach events having a negative impact on consumer sentiment.[7] These breaches come at a cost to Australians, with estimates that between $3-4 billion has been lost to scams in 2022 representing a 300% increase since 2020.[8] As such, modernisation of privacy laws should achieve an overall net benefit to Australia.

The commercial and operational opportunities associated with these proposals should not be overlooked. Expansion to the scope of PI covered under the Act, coupled with record keeping obligations, will require entities to systematically understand the extent of data held across their organisations. Identifying and qualifying data assets is a powerful and important step to extracting value from data, including to differentiate from competitors, make better business decisions, inspire new products and reimagine service delivery. Further efficiency gains can be realised for organisations that can implement effective data minimisation practices, such as removing redundancy and achieving associated cost savings. Typical observations based on our experience include - systems storing PI however there are no users, storage locations where physical files are archived indefinitely, and instances where PI is duplicated across repositories.

A need for harmonisation of privacy-related laws and regulations operating across Australia

There is opportunity to be realised if Australia can move towards a more integrated and seamless digital and data regulatory framework. We welcome the Report's proposals regarding the initial steps to achieving increased simplicity and consistency of privacy-related obligations in Australia. PwC recommends continued work and ongoing focus in this space to enable a more seamless digital economy, to simplify what privacy means to individuals and to reduce compliance burden.

Organisations need to navigate complex legislative and industry frameworks to be confident in the design and operationalisation of privacy compliance measures. In addition to the Act, this typically includes consideration of international privacy regimes, differing privacy laws across Australian jurisdictions, surveillance and workplace monitoring laws, health records acts and, more recently, privacy safeguards set out in the Consumer Data Right (CDR) and Data and Availability Transparency Act (DAT). Further complicating compliance strategies, privacy obligations also often vary for consumers, employees and contractor segments. Alignment of legislative and industry frameworks (including underpinning guides, tools and templates) should be prioritised as a means to progress Australia's privacy agenda with greater velocity.

For example:

- Organisational accountability proposals relating to record keeping of *purposes* should consider leveraging existing practices, like the Office of the National Data Commissioner's (ONDC) data cataloguing pilot program, which seeks to develop data inventories for 20 per cent of Australian Government agencies.[9]
- Privacy Impact Assessment guidance and templates produced by the OAIC could better align with equivalent material from other Australian jurisdictions to improve consistency and interoperability.

---

[6] https://www.dfat.gov.au/about-us/publications/trade-and-investment/business-envoy-april-2021-digital-trade-edition/innovating-australias-digital-economy
[7] https://www.pexa.com.au/content-hub/data-breaches-impacting-australian-consumer-sentiment/
[8] Address to the AFR Banking Summit | Treasury Ministers
[9] ONDC launches pilot project for the Australian Government Data Catalogue

Given this review is occurring concurrently with the development of related strategies and reform processes, there is an opportunity to ensure these changes are complementary and not siloed.

It is challenging for Australian organisations to navigate an overly complex data retention regulatory environment - this is a key issue for reform of the Act to address. Australia's data retention regulatory landscape is complex, with a range of obligations relating to minimum and maximum retention periods. For example, both the Australian Prudential Regulation Authority (APRA) and the Australian Securities and Investment Commission (ASIC) require financial records and client advisory notes be retained for seven (7) years, whilst the Australian Taxation Office imposes a five (5) year retention period on tax statements and payment receipts. As it stands, there is no central repository containing details of the various regimes in operation across Australia meaning that organisations are essentially 'left to their own devices' in deciphering this complex puzzle. In our experience, this has contributed to data being over-retained and presents a significant risk to individuals, as seen in recent large scale data breaches. It is our belief there is scope for the creation of a Federal Government-led data retention repository detailing the provisions of relevant regimes, to be updated as required to help alleviate hurdles around PI retention and disposal. Another key driver has been the rapidly decreasing cost of storage and the potential of monetisation of data. Only now, after recent large scale data breaches, has the liability of retaining data beyond its predefined retention period really come to the fore.

The practical challenges and potential burdens that organisations may face as a result of these reforms, and the importance of leadership.

Given the sweeping and comprehensive nature of the proposals, there will be significant practical challenges for organisations to overcome. We expect organisations will need time, skills and comprehensive guidance to implement processes and measures in areas of higher complexity like those relating to consent, fair and reasonableness tests, privacy rights requests, de-identification and disposal - some of these are enduring challenges faced by organisations that we expect will persist. Implementation of technical and organisational measures will be further compounded for organisations that operate complex data architectures, such as those reliant on legacy systems (which are costly to replace) and supply chains (for PI processing and hosting). Emerging technologies including automation, advanced analytics, artificial intelligence and facial recognition will also need clear guardrails in order for organisations to meet principles around transparency and explainability without stifling innovation.

These reforms will lift the privacy benchmark for the economy and compliance will require organisational re-prioritisation and investment. In an environment of economic uncertainty, we expect organisations will continue to take a risk-based and prioritised approach when addressing privacy compliance matters. We are observing some sectors adopt data risk practices in line with Prudential Standard CPS230 Operational Risk Management (which comes into force on 1 January, 2024), whereby Australian Prudential Regulation Authority (APRA) will require regulated financial sector entities to have a comprehensive view of their operational data risks and to implement controls in accordance with risk appetite. Noting the number of proposals, this legislative reform process may consider a phased approach to alleviate pressures on the economy, as was the case with critical infrastructure reforms, which took shape across two tranches of reform.

Leadership will be needed to set clear direction and pave the way for organisations. Recognising the extensive set of proposals, we suggest comprehensive communication is required to provide organisations with a clear set of directions to follow and the essential practices to be prioritised. For example, the Essential Eight, published by the Australian Cyber Security Centre (ACSC), has been an effective tool to educate the market on what is 'essential' to mitigate a cybersecurity incident. Furthermore, we recommend the OAIC set out a roadmap prioritising the legislative and regulatory actions that would deliver the greatest benefit to the community when the outcomes of this review are finalised (recognising the volume of various guidance, clarifications and lists recommended by the proposals). This would help guide the Federal Government in introducing prioritised tranches of legislation to reform the Act. We would expect the following areas to be of highest priority: harmonisation and alignment with emerging regulatory frameworks; tools to accelerate accountability proposals; and technical guidance for complex areas (such as consent, de-identification and disposal, and other areas outlined above). Finally, leadership in setting direction and regulating the market may take many forms, but should consider the role of the Australian Government, regulatory bodies (OAIC and others) and industry representatives. For illustrative purposes, in the financial services sector, Prudential Standard CPS234 Information Security acts as the binding set of directions to be followed and APRA plays an important role as an independent authority to supervise the sector.

Our key submissions

What information should be protected and who should protect it?

We generally support proposals around the expanded scope and definition of PI as a foundational pillar to the effectiveness of the Act. This should be delivered through instruments which are flexible (not reliant on legislative processes) to ensure the Act is future proof and able to adapt to new and emerging issues. By broadening the definition of PI, organisations will be encouraged to re-evaluate the PI they hold and move towards data minimisation (such as the adoption of accredited digital identity services to reduce the amount of sensitive PI collected). However, given the broad definition of PI pursued, directions will be needed to ensure protections remain prioritised on the situations that represent the greatest risk of harm to individuals (e.g. handling of financial PI for vulnerable individuals, in the context of leaked identity records, may need additional protections).

The proposed expansion to cover inferred and generated PI is likely to cause practical challenges in relation to consent and collection notice requirements that may now be triggered. Similarly, further consideration should be taken in relation to proposals relating to 'de-identified' data.

We support proposals to better protect employees and have observed many public and private sector organisations already choosing to apply privacy measures to maintain trust (e.g voluntary data breach reporting) and meet global privacy laws. Removal of the small business exemption would need to be managed appropriately to accommodate the large and diverse population of small businesses that would be impacted.

What privacy protections should apply?

In a digital world, effective cyber security is essential to protecting PI. While we support proposals aimed at uplifting the protection of PI, such steps must be considered with respect to the practical technicalities involved and potential burden to organisations in terms of cost, resourcing and skills in a difficult economic environment. The current data retention environment is complex and, we submit, is a key issue to be addressed. We agree with proposals relating to guidance clearly articulating what reasonable steps may be undertaken to destroy or de-identify PI, in the context of today's digital landscape where destroying PI can be technically difficult to implement.

In principle, we support the proposed changes to consent and collection notices, including appropriate usage of standardised templates and layouts. It is important to flag that not all Australians will proactively engage with the privacy rights they are given, and as such, considerations are needed to maintain inclusion and mitigate unintentional impacts (by way of example, many Australians choose not to engage with superannuation options even though it is in their best interests to do so). We are supportive of proposals that move towards and better enable the protection of vulnerable individuals who may experience greater risks of harm through the use of their PI.

We agree there is value in organisational accountability measures (which relate to the recording of the purposes and to expressly require entities to appoint a suitable responsible person for privacy). We agree that the introduction of a 'fair and reasonable' test will provide confidence to individuals however there are practical challenges to further consider.

How should breaches of privacy be enforced?

Reforms of the Act's enforcement regime should be designed to promote certainty and clarity, and be targeted for maximum impact from a compliance perspective. We agree with proposals that will enable appropriateness of resources and funding to achieve this outcome. Further consideration should be given to the establishment of a multi-regulator regime (similar to the Security of Critical Infrastructure regime) to leverage the knowledge and resources of established industry-specific regulators.

We generally support reforms to the civil penalty regime to establish more targeted and flexible enforcement measures and support proposals to clarify the existing civil penalty provision. Further, we are supportive of establishing an avenue for individuals to personally take action for relief where there has been a certain level of interference with their privacy. However, consideration should be given as to what standard should apply to the individual right of action when there is an expansion of civil penalties for lesser breaches. As mentioned above, it is important to recognise that these legal routes may not always be meaningfully accessible across individuals in our diverse community.

We support adjustments to the Notifiable Data Breach (NDB) timeline to 72 hours, however it may be prudent to reinforce guidance to address situations where there is insufficient information to determine if the data breach is eligible for notification. We support proposals to harmonise data breach and cyber incident notification schemes to simplify reporting obligations and burden for entities in the midst of breach incidents.

Our response to the proposed privacy reforms

We have considered the 116 proposals presented in the report and, where applicable, have presented key advice and recommendations for consideration. Our responses are aligned to the Attorney-General Department's three key questions.

Question 1 - What information should be protected and who should protect it?

As digital systems continue to evolve and increasingly underpin the way almost all organisations operate, PwC agrees the scope of information protected under the Privacy Act (the Act) requires amendment to meet the needs and expectations of the community when it comes to the use, handling and protection of PI. This is no small feat however, as the sum of the proposed changes relating to the scope of PI and APP entities covered under the Act would result in substantial additional compliance activity across Australian organisations. Captured organisations would require resources and investment to re-assess the scope of PI held, classify this data accordingly, perform impact analyses and operationalise changed privacy protections. While this presents an opportunity for organisations to ensure more effective and accurate oversight of PI is maintained and for organisations to revalidate data minimisation practices, reforms should take into account the time, skills and resourcing required to comply with such changes.

PwC supports the development of prescriptive, adaptable and useful guidance to help organisations work towards and remain compliant with the Act. This includes the adoption of mechanisms whereby guidance could be modified quickly and easily to meet changing needs, where appropriate bypassing the time-consuming legislative process. The OAIC should proactively address areas where clarity is needed and where complexity in implementation is likely to arise, like how to navigate consent activities being triggered for inferred and generated PI, and to manage the risks of privacy fatigue. Research shows privacy fatigue "brought on by casual data breaches and the complexity of online privacy control, can reduce users' attention to privacy issues",[10] having a stronger impact on privacy behaviour than privacy concerns do, although the latter is widely regarded as the dominant factor in explaining online privacy behaviour.

These proposed changes in aggregate, including the removal of the employee records exemption and small business exemption, would bring a significant number of new entities and data sets into the scope of the Act. If implemented, it will be important that an appropriate regulatory enforcement strategy be adopted, ensuring the OAIC's enforcement resources are prioritised to where it matters most for the Australian community.

Definition of PI

PwC supports Proposals 4.1 and 4.2, recognising that clarity for organisations will be a key pillar and foundational to effectiveness of the Act. Having clear guidance that is adaptable and useful is necessary for the transition to an updated Act. PwC supports the proposal of a more structured definition of PI. The more prescriptive nature of a new definition would benefit APP entities, including small businesses if the exemption is lifted. This includes Proposal 4.9, where PwC agrees that 'genomic' information is a category that should be captured as sensitive information under the Act.

A non-exhaustive list of PI types would be advisable but must add value in terms of helping organisations understand whether information will be captured and regulated as PI. This should focus on practical guidance that addresses more obscure or unfamiliar PI types, like metadata, audio recordings, physical video footage and surveillance data, segmentation data about an individual, online identifiers, browsing history, or device data. A list calling out basic PI types, like names and email addresses, would add little value for organisations. This proposal also represents a significant shift towards alignment with the GDPR and other international legislation - and if implemented, we suggest leveraging indicative lists of PI types that already exist in other jurisdictions.

While data is increasingly being used to profile individuals for targeted advertising and other purposes, this profiling also occurs maliciously, with threat actors adept at exploiting PI. Increasing the scope of what is considered to be PI reflects trends we are seeing in the public domain, whereby seemingly innocuous information is being combined to create personally identifiable information, which is then used for malicious purposes.[11] For instance, online identifiers and exposure of IP addresses are being used for credential stuffing.[12] These examples of PI misuse need to be considered in the expanded definition.

[10] The role of privacy fatigue in online privacy behavior - ScienceDirect
[11] Identity theft | Cyber.gov.au
[12] FBI: Beware Residential IPs Hiding Credential Stuffing - Infosecurity Magazine

By broadening the definition of PI, organisations will be encouraged to re-evaluate the PI they hold. To promote data minimisation, consideration should be given to the use of digital identity services like MyGovID or an alternative form of digital citizen identity. These services minimise the amount of PI held by organisations as it is outsourced to accredited identity providers. While the ecosystem is still in early development, it will help provide improved security and privacy as it matures. With discussions ongoing in relation to a national digital identity and associated legislation, there is an opportunity for its development to be aligned with the reforms at hand.

Taxonomy of data classes and prioritisation

Given the broad definition of PI, there is a question as to the relative priority of how PI will need to be protected. For example, is identity information more sensitive than health and medical records and how do these compare to financial account details and geo-location data? Without clear prioritisation across industries, organisations risk taking inaction due to the size and complexity of the challenge.

Directions will be needed to ensure organisations prioritise safeguards in the areas that represent the most harm for individuals. Three main considerations should inform where to prioritise PI protections:

- Type of data - the nature of the data itself warrants the treatment of it with care, e.g. ethnicity, health, biometric information;
- Type of individuals - the data is about individuals who are vulnerable, e.g. minority groups, children; and
- Contexts - the data concerns higher risk situations, e.g. data sharing, data breaches and emerging technologies such as Artificial Intelligence.

Individually, these considerations are of equal importance. However, if more than one of these considerations are present, the risks of harm are increased (e.g. health information of individuals belonging to minority groups), with the highest priority being where all three considerations exist.

Broad range of PI used to harm individuals

In August 2021, the OAIC published its notifiable data breach report and drew attention to impersonation fraud, which involves a malicious actor impersonating another individual to gain access to an account, system, network or physical location. Information Commissioner Angelene Falk said: "The growth of data on the dark web unfortunately means that malicious actors can hold enough PI to circumvent entities' 'know your customer' and fraud monitoring controls".[13] A malicious actor can steal a person's identity by using a small amount of hacked PI, connecting this with other public sources, like social media accounts which may include date of birth, photos and information about a person's family.

In Australia, it is estimated that between $3-4 billion was lost to scams in 2022, a 300% increase since 2020.[14] Further data published by the US Federal Trade Commission (FTC) stated US consumers lost almost $8.8 billion to fraud in 2022, an increase of more than 30% over the previous year. *Imposter fraud* is the leading cause for consumer fraud in the US.[15]

Collection, Inferred and Generated Data, and De-identification

Clear guidance will be required in relation to the interpretation of the proposed expansion to inferred and generated data to mitigate practical challenges that may arise. With reference to proposals 4.3 and 4.9(c), amending the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information, will come with practical challenges around the collection notices and consent practices that need to be adopted. For inferred or generated information, many organisations are not currently adopting collection notices or practices for this type of data (such as marketing segmentation processes and hardship flags). Further, under the proposals, Artificial Intelligence or Machine Learning (AI/ML) activity that generates new PI related to a person could require collection rules to be triggered. Specific to proposal 4.9(c), sensitive PI inferred from non-sensitive PI could trigger new consent requirements.

Without defined parameters, the proposed amendment could trigger large-scale consent requirements for organisations related to sensitive information, which may not be practical or proportionate. New collection and consent notices across multiple streams may lead to 'privacy fatigue', whereby consent activity becomes less meaningful or adversely impacts benefits that can be derived from using data where consent is not given. To this end, a focus of the reforms should be placed on balancing compliance costs and real benefit to individuals or the public. As such, further guidance on the practical implementation of this proposal is recommended.

[13] https://www.oaic.gov.au/newsroom/data-breach-report-highlights-ransomware-and-impersonation-fraud-as-concerns
[14] Address to the AFR Banking Summit | Treasury Ministers
[15] New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022

Sample Scenario

Retail Co is an Australian small business selling clothing apparel. It holds PI of its customers, including name, address and transaction history. It does not collect sensitive data as it is not part of its primary activity or function. Every year, Retail Co organises targeted sales campaigns during the holiday season, including for Christmas, Easter and Lunar New Year. Through a customer's purchase patterns, potential inferences could be made about their racial or ethnic origin and this is defined as sensitive data under the Act.

Retail Co does not have technology capabilities to reverse engineer spending patterns to identify its customers, and does not have current means to obtain consent from its customers. It will need to consider the compliance requirements that come with holding and managing sensitive PI. However, as the proposed amendment to collection of sensitive information under the Act does not qualify to what extent an 'inference' can be made, nor applicable parameters, Retail Co may be in breach of both the Act and the requirements of APP 3.2 should it not take concrete steps to address this issue.

PwC supports having clearer guidance on de-identification and anonymisation of PI (in relation to Proposal 4.5) and cautions the introduction of what may appear to be another tier of data covered by the Act, being 'de-identified' PI. We agree with the overall concept of ensuring that de-identification is properly carried out to minimise the risks of re-identification. We understand the intent of the proposed amendments to APP 11.1 (with reference to Proposal 4.6 and 21.4), which would require APP entities to take reasonable steps to protect de-identified information. However, there is concern that the introduction of a new tier of regulation on information that is not PI, being 'de-identified information', would introduce unnecessary complication to an already complex area. De-identification of PI is an important process undertaken by organisations to allow the free and open use of valuable data sets for analysis and insight generation and introducing new obligations that apply to this type of data runs the risk of increasing legal and regulatory barriers. We recommend reforms be focussed on ensuring the de-identification process is properly undertaken to protect individuals. We believe this strikes the appropriate balance between tempering regulatory burden and providing reasonable protections to an individual.

We note there has been some investigation of use and disclosure of 'anonymised' data whereby a published dataset was able to be re-identified by university researchers.[16] This incident was investigated by the Office of the Victorian Information Commissioner (OVIC). However, the conclusion of OVIC concentrated on whether the information was truly anonymised in light of other publicly available dataset. Further, as far as PwC is aware, there has been no major incident in Australia where large quantities of de-identified data has been misappropriated and subsequently re-identified by a threat actor.

Power to make an APP Code

PwC is supportive of Proposal 5.1 and, in general, advocates mechanisms which can be utilised to ensure the Act is future proof, scalable and tailored to capture and adapt to issues applicable to new and emerging sectors of the economy. In PwC's experience, large variation exists across the economy in terms of data collection, data management, data governance and data use practices depending on the relevant sector. For example, a data rich digital platform should be regulated differently from a large resources company. Consideration should be given to whether codes should be utilised more often and passed down by relevant sectoral regulators (similar to rules under the Security of Critical Infrastructure (SOCI) legislation), rather than relying on industry bodies to lead this process. Any such process must have appropriate consultation and engagement processes in-built, but the lack of use of the codes under the existing regime illustrates there is room for improvement. We have addressed this further in Question 3.

Small business and employee exemptions

Removal of the small business exemption (Proposal 6.1) needs to be managed appropriately to accommodate the large and diverse population of small businesses that would be impacted. A summary of the anticipated and wide-ranging impacts is outlined in the diagram below.

[16] Travellers' movements and identities at risk by public release of "anonymised data"

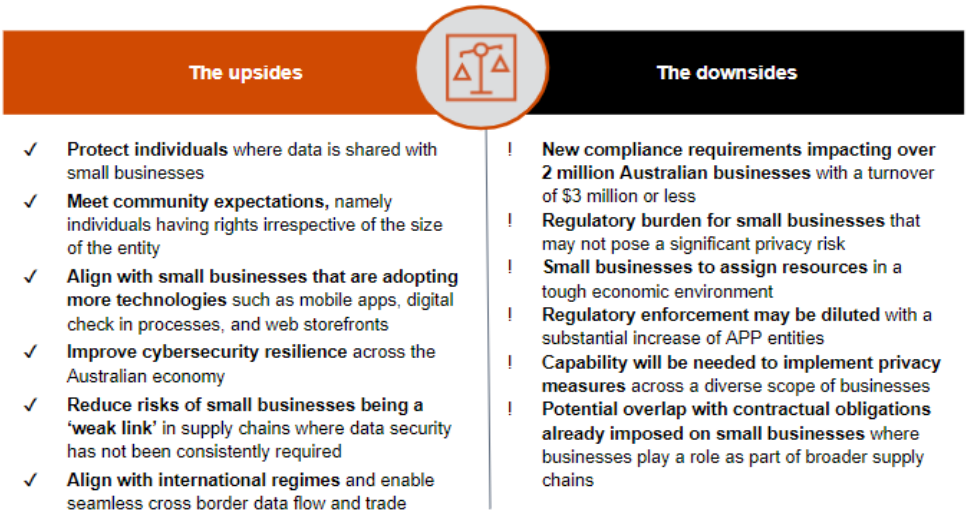


Figure 1.2[17]

Generally speaking, the aggregate privacy risk in the small business community is relatively lower when compared to large organisations and government institutions in Australia. PwC appreciates a risk-based approach has been proposed to enable proportionality and practicality for small businesses, whereby a different privacy baseline would be mandated depending on the level of privacy risk tier. To this end, a self-service risk triage engine or decision tree would help small businesses determine their risk category and resulting set of baseline requirements. We recommend careful consideration be taken as to how these standards would apply to help avoid unintentional legislative complexity, for example, the provision of explicit exemptions in the Act for privacy principles that would not apply to small businesses.

PwC agrees with the assertion that support mechanisms will be critical for the success of this proposed reform. We submit the following considerations could be taken into account:

- Clear and prescriptive guidance - translating the privacy principles into a baseline set of requirements and the use of plain language and easy-to-follow steps.
- Free and accessible resources - template privacy policies, collection notices and data breach playbooks available at no-cost to small businesses to provide clarity and improve quality of outcomes.
- Education and awareness - a change management strategy to communicate obligations across the large population of small businesses (leveraging existing industry associations and networks to communicate changes and enable access to resources).
- Language and translation - any materials produced would need to be accessible across a diverse and multicultural community of small business operators.
- Transition period - a grace period should be considered, recognising the time needed to support and educate small businesses on new privacy obligations.
- Incentive-based strategies - to encourage small businesses in their adoption of privacy requirements. These could include financial incentives (benefits and grants), alignment to government procurement processes (where small businesses form part of the supply chain) and public recognition of small businesses as industry leaders or role-models in privacy management.

PwC supports Proposal 7.1 recognising this as an important measure to protect the employee workforce. PwC observes that many public and private sector organisations already apply privacy measures for their employees to maintain trust (e.g voluntary data breach reporting) and to meet obligations imposed for multinational corporations. The proposal to add enhanced privacy protections to private sector employees is a step in the right direction and largely shadows the employee rights of GDPR and other international privacy regimes. It also presents an opportunity to help unwind Australia's patchwork of privacy laws to achieve an equity of privacy rights across the community and to simplify privacy obligations. By way of example, contractors may have greater protections compared with employees (of the same entity) as a result of the employee records exemption; and an employee record may fall into the scope of the Act's notifiable data breach regime where it includes Tax File Numbers. We agree it is important for the Attorney-General's Department to continue the consultation process suggested (with employer and employee representatives), taking note of complexities around how protections are to be legislated, including how privacy and workplace relations laws should interact.

[17] https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/latest-release#key-statistics

Question 2 - What privacy protections should apply?

As previously mentioned, a key objective of this reform process should be striking the right balance between protecting individuals' privacy, and ensuring reforms are not overly burdensome on captured entities. We note that while there will always be a general compliance cost involved with a regime of this nature, it is important to highlight these costs are not always incurred for compliance sake - good privacy legislation can target those costs to investments that protect individuals and also enhance organisational value.

Improvements to an organisation's data governance and PI management processes can create a significant competitive advantage and value for an organisation. This is not just because organisations offer a compelling value proposition to consumers where their PI management is well structured and secured, but also the reality that proper management and categorisation of data would allow organisations to make better use of their current and future data holdings. Ultimately this enables organisations to draw insights and derive value from data holdings, which would not otherwise be possible. By targeting reforms in these areas, value-creating activities can be progressed with the backing of a compliance objective. Such value generation ultimately benefits society more broadly, as employees, shareholders, customers and other stakeholders derive benefit from enhanced privacy protection.

In assessing harms that may arise following misuse or loss of PI and the required protections to mitigate them, there is first a need to acknowledge that privacy harms vary depending on an individual's circumstance and risk profile. Harms can also vary in their severity - an incident that occurs at scale is likely to have a more significant impact on the population than a discrete incident impacting an individual. People from minority groups also face higher risks of re-identification given their PI may present as an outlier, making it easier to combine it with externally available data and to identify and target them. This potentially exposes minority groups to greater risks of marginalisation or being specifically targeted due to personal factors like sexual orientation or cultural background. Therefore, reforms must consider vulnerable cohorts in our society and take steps to prevent exploitation of individual traits that could lead to targeting via collected data.

As we continue through a period of global uncertainty and instability, the protection of data and information (including PI) is of paramount concern to nations. Poor data management and subsequent data breaches can have a catastrophic effect on individuals, organisations and governments. There is no doubt the protection of data assets is more than just a concern for individuals. Data breaches have rippling effects that cascade through the economy, as has been experienced acutely in Australia in the past year. Therefore, we submit that there is an opportunity via the reform process to articulate the public benefit of privacy protection to both APP entities and the community.

Security, retention and destruction

Cyber security

In a digital world, effective cyber security is essential to protecting PI. While we support proposals aimed at uplifting the protection of PI, such steps must be considered with respect to the practical technicalities involved and potential burden to organisations in terms of skills, cost and legacy systems. Furthermore, with the development of the 2023-2030 Australian Cyber Security Strategy (the Strategy) occurring concurrently, there is an opportunity to ensure that these reforms and the Strategy are complementary, do not create duplicative obligations and provide clear advice to help organisations better protect PI. Likewise, as the national discussion about citizen identity continues to evolve, steps must be taken to ensure privacy and security are 'baked in' to any proposed legislation, operating in congruence with the Act and the Strategy to create a more harmonised privacy and security ecosystem as opposed to siloed regimes. Thus, we are supportive of Proposal 21.2 and its intention to establish baseline privacy outcomes that will align with and be informed by the Strategy.

In relation to cyber security, it is important to note there is no silver bullet solution. Unfortunately in the digital environment, data breaches are inevitable and therefore, these reforms need to reflect the dynamic nature of cyber security and emphasise the need for best practice. Some sectors, like the 11 captured by the SOCI Act and financial services, are already highly regulated, with cyber-specific obligations a key focus. However, other sectors, like retail, real estate and not-for-profits, which do not have cyber-specific regulatory obligations, may not have the same level of cyber maturity, yet are also captured by the Act. Hence, there is significant variation in the cyber maturity of the organisations the Act impacts and, as part of these reforms, adequate time to implement cyber uplift and build maturity should be considered, especially if amendment to APP 11.1 is undertaken.

Similarly, this principle could be reflected in Proposal 21.3, which relates to the enhancement of OAIC guidance in relation to APP 11. We recommend such enhancement should acknowledge and reflect that 'reasonable steps' is not a one-size-fits-all measure and that, in the event of a breach, the unique circumstances of an impacted organisation should be taken into account. These considerations would not only help prevent significant burden for less mature organisations and ensure OAIC discretion comes to the fore, it would encourage organisations to continually uplift at a sustainable pace. To this end, it would also be advisable that any cyber security guidance developed by drawing on the Australian Cyber Security Centre's (ACSC) technical advice should be, at a higher level, general, and underpinned by specific guidance tailored to different audiences or sectors, for example, small and medium enterprises, retailers, real estate, not-for-profits etc.

Data retention

Currently, Australian organisations exist in a data retention environment that is piecemeal and significantly complex - this is a key issue for reform of the Act to address. There are a myriad of data retention regimes operating across a range of sectors in Australia's federal, state and territory jurisdictions, with legal obligations for some data to be retained for many years. In our experience, uncertainty over data retention obligations has resulted in data being over-retained, which is exacerbated by the practical difficulties of separating data at an organisational level and technology challenges in disposing PI.

It is our strong belief that there should be a 'single source of truth' for APP entities navigating the complexities of data retention and submit there is scope for the creation of a Federal Government-led repository detailing the provisions of relevant regimes, to be updated as required. We are supportive of Proposal 21.6, which would require the Commonwealth to undertake a review of all legal provisions that require retention of PI to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of PI. By way of example, at a state level, retention and disposal authorities prescribe a 50 to 75 year retention period for patient information records, while the Australian Code for the Responsible Conduct of Research recommends a 15 year retention period for clinical trial data. We submit that such a review could result in the establishment of a data retention repository, as previously noted, which would assist organisations in achieving greater clarity and certainty in relation to their data retention obligations. Likewise, we are supportive of the Commonwealth, states and territories working together to better harmonise existing regimes, which could be captured by Proposal 29.3 and its proposed formation of a federal, state and territory working group. This will help to ensure future data retention policies across federal, state and territory jurisdictions are not duplicative or contradictory.

In addition to the above, organisations will also need to have a clear understanding of how long PI should be kept, and at what point it needs to be disposed of, as part of an effective and holistic data minimisation strategy. We anticipate organisations with large and complex PI data flows will need time to adopt Proposals 21.7 and 21.8 in relation to establishing and publishing PI retention periods. However, we have observed entities already taking steps to define PI retention periods.

Another issue, which is often overshadowed by a focus on data retention periods, is the storage of multiple copies of the same data across an organisation's systems and repositories. Some of these repositories can be particularly vulnerable to exploitation and the data more easily accessed by malicious actors, creating an additional risk beyond retention. There is an opportunity for the OAIC to provide explicit guidance to help organisations minimise the spread and footprint of their data.

Destruction

PwC supports Proposal 21.5, which would require the OAIC to enhance its guidance in relation to APP 11.2 to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify PI. There are wide ranging practices being pursued by APP entities in efforts to meet these obligations, such as logical deletion, putting information 'beyond use', masking and hashing. Additional clarity on what constitutes 'reasonable steps' in the context of complex data environments (such as cloud services, legacy systems, and outsourced providers) can help APP entities to address this important step in their holistic data minimisation strategies.

Further, our recently published report 'After Life: Critical Infrastructure and the e-waste data threat', notes there is scope for the OAIC to provide specific guidance beyond the existing 'Guide to Securing PI' in relation to the secure disposal of redundant devices for organisations captured by the Act, which could be enhanced further to provide greater clarity in relation to specific data destruction.[18] The report highlights the significant data and cyber security threats e-waste and its insecure disposal pose to Australian organisations, with the data stored on these devices and their components potentially containing sensitive PI that, if in the hands of malicious actors, could result in significant cyber and data breaches. Such guidance could include key steps that organisations should undertake to ensure their e-waste is securely sanitised or destroyed. Such guidance would be of particular assistance to small and medium enterprises, which have more limited resources and expertise to support secure disposal practices.

Fair and reasonable test

The introduction of a general requirement of a 'fair and reasonable' test in Proposal 12.1 may result in practical challenges in its operationalisation. Introduction of a 'fair and reasonable' test will require a level of judgement in its interpretation and require mechanisms for the 'test' to be applied across a wide range of circumstances, from simple day-to-day business activity to extremely complex solutions. This may lead to organisations operating with a level of uncertainty in relation to PI, as their assessment of the test could potentially be incorrect at any given point. A test of this nature may also have the potential to undermine agreements between individuals and APP entities. For example, if a fully appraised individual consented to a particular use or disclosure that was unorthodox or innovative, there may be a possibility that a court would find such use or disclosure has breached this test of 'fair and reasonableness'.

[18] Critical infrastructure and the e-waste data security threat

We agree that this proposal will help to ensure entities' handling of PI is within individuals' reasonable expectations and is not harmful, giving Australians a level of confidence in how their PI is being used. If a 'fair and reasonable' test were to be introduced, prescriptive and specific guidance should be made available to help organisations interpret the meaning of 'fair' and 'reasonable' in the context of their business operations. We recognise that a number of factors have already been identified and note these as being reasonably in line with 'data ethics' principles pursued by some APP entities already. These include factors relating to whether the individual would reasonably expect this PI processing and if the risks of harm are proportionate to the benefits. The adoption of a 'fair and reasonableness' test may be performed together with privacy impact assessments.

Organisational accountability

PwC agrees with Proposals 15.1 and 15.2, which relate to the recording of the purpose for which data would be collected and expressly require APP entities to appoint or designate a senior employee responsible for privacy within the entity. Recording the purpose for collection, use and disclosure of PI would encourage organisations to take a deeper and more discretionary view of the data they hold. A positive impact of this would be that organisations consider data minimisation and privacy-by-design principles, developing a clearer view of redundant data and collection that does not contribute to the organisation's purpose. To ease the compliance burden, prescriptive legislation should be accompanied by tools and templates to help organisations achieve compliance. There is potential for this proposal to promote data minimisation due to the natural self assessment which will occur when collecting data. There is an opportunity to align with other data inventory standards in Australia, such as those used as part of the Data Inventory project commissioned by the Office of the National Data Commissioner (ONDC) to enable data sharing initiatives in the public sector.

While we support Proposal 15.2, we note that APP entities must ensure that the individual responsible for organisational privacy is someone who is experienced and willing to take on responsibility for privacy. Furthermore, such an individual should be well supported and have direct reporting lines to the very top of the organisation, given privacy must be considered a key factor in organisational operations. As part of the reform process, governance guidelines should be provided as to the type of skills, training and experience needed to take on the role. This is especially pertinent given the interlink between this proposal and the small business exemption. Not every organisation has a resource available who is both willing and capable of taking on this role. In some cases, organisations would need to search for the required talent, which is a limiting factor.

Privacy policies and collection notices

PwC supports Proposal 10.1 to introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place. Such a step essentially brings the existing OAIC guidance into the legislation. On this basis, we agree and acknowledge the importance of ensuring that public and consumer facing documentation, a core component to transparency, should be expressed in a manner that is clear and understandable for most people. In our experience, any organisations do not currently provide proper collection notices and merely refer to their privacy policy via hyperlink. This notice is an important part of the PI lifecycle and should be provided as soon as possible after collection and, where possible, at the time of collection, in plain English drafting.

PwC supports Proposal 10.3, that standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. Standardised templates and layouts could be useful in aiding interpretation of privacy policies and collection notices. However, terminology may differ across industries and sectors. As a result, any centralised definitions or terminology would need to be clearly defined and subject to consultation with relevant sectors. Further, whilst uniformity is important, it is vital to ensure it does not result in a lack of engagement with the policy of organisations. There may be a risk that organisations could outsource compliance to standardised templates without meaningful engagement. It is important that any privacy policy and collection notice regime is supported by appropriate enforcement measures for the OAIC in order to better ensure compliance.

Consent and online privacy settings

PwC supports Proposal 11.1, that the definition of consent be amended to provide that it must be voluntary, informed, current, specific and unambiguous. This would essentially bring existing OAIC guidance into the legislation. In our experience, many organisations already approach consent in this manner. However, there is an opportunity to provide greater clarity within legislation that displaces the concept of implied consent. If so, the definition should state that consent must be express. If not, guidance should be issued to show where the amended definition would apply in the context of an implied consent situation.

In principle, PwC supports Proposal 11.2, that OAIC could develop guidance on how online services should design consent requests. Uniformity and guidance can be extremely useful tools for organisations to ensure compliance. However, any guidance of this nature should ensure it does not inadvertently result in organisations failing to engage properly with the process. There is little value in organisations relying on template guidance to avoid actually considering the nuances of their individual situations and requirements. Hence, the introduction of the proposal could be paired with an appropriate enforcement regime to encourage consideration of individual circumstances.

In principle, PwC supports Proposal 11.3, to expressly recognise the ability to withdraw consent and to do so in a manner as easily as the provision of consent. It is not always possible to align a consent withdrawal procedure with the consent giving procedure. Due to process flows and the realities of technology, it is often more difficult to withdraw consent than it is to give consent. As a result, we recommend this proposal include the ability to withdraw consent in a manner that is reasonably accessible in the circumstances. Withdrawal also should not result in an instantaneous obligation to cease using PI - reasonableness parameters should be implemented to recognise the realistic nature of the task of processing withdrawal requests, especially small and medium businesses.

Further, clarity should be considered for instances where a withdrawal may impact commercial arrangements and relationships. For example, if a customer obtains services that rely on the use of their PI for a discount based on a longer term commitment, the right to withdraw consent for the use of that information would undermine the contract between the parties and the pricing or discount model put into place.

People experiencing vulnerability

In principle, PwC supports Proposals 17.1 and 17.2 and affirms that it is a step in the right direction towards protecting vulnerable individuals who may experience greater risks of harm through the use of their PI. Organisations should be able to distinguish between a vulnerable individual's ability to give informed consent based on their unique circumstances, personal characteristics and the validity of the consent itself. In this context, privacy harms facing vulnerable individuals are further exacerbated because of underlying characteristics and circumstances unique to them. These may include language barriers leading to an inability to give informed consent, greater risks of marginalisation, or being specifically targeted for sexual orientation or cultural background.

This proposal may go beyond a non-exhaustive list of risk factors and tailored consent mechanisms, to also set out the controls to be considered in the handling of PI to protect vulnerable individuals. This should build on Free and Prior Informed Consent (FPIC), the Disability Discrimination Act 1992 (DDA), the Closing the Gap Framework and ISO 29184 for accessibility practices (such as multilingual consent notices and options for those with visual impairments).

Sample Scenario

Val is a senior citizen who belongs to a minority group and her ability to speak and understand English is rudimentary. XYZ Co is a local retail outlet operating in her town and decides to run a campaign involving promotions and cashbacks offered to customers who use their rewards card for every transaction. Val signs up for the rewards card program and provides her PI. Owing to her limited understanding of both the English language and the legalities around processing of her PI, Val may not have fully understood what she was consenting to, nor the privacy risks involved.

XYZ Co suffered a data breach and Val's PI was stolen. Although XYZ Co issued a circular to all customers on how to protect themselves, including changing passwords, Val, who is not technology fluent, did not take any mitigating steps to limit her exposure. As a result of these specific underlying characteristics, Val is a vulnerable consumer and is at greater risk of targeted and repeat cyber crimes. Notably, even if XYZ Co had de-identified Val's data, as a person from a minority group, her risks of re-identification are higher given her PI may present as outliers, making it easier to combine them with externally available data and subsequently identify and target her.

Controls measures to be considered to protect the PI of vulnerable individuals may include:

- training employees to recognise vulnerable consumers and the disproportionate privacy harms they face;
- offer additional assistance at the point of signing up (e.g., an interpreter or easy to understand infographics) to ensure informed consent is given, and that the customer knows whom to contact in the event of an emergency;
- internal policy that does not allow for the use, disclose and storage of PI of vulnerable consumers for any other purpose, nor beyond the promotional campaign;
- a dedicated hotline that prioritises reaching out to vulnerable consumers and assisting them in real time to change their passwords and take other mitigating steps;
- tailored support plans to include counselling and/or professional mental health support in the event of a breach.

Question 3 - How should breaches of privacy be enforced?

Under the current regime, the OAIC's responsibility to supervise, enforce, educate and monitor is significant, and this is likely to expand in scale as a result of proposed reforms. By way of example, removal of the small business exemption would result in a spike in the number of businesses the OAIC is required to regulate, noting 93% of Australian businesses have a turnover of less than $2 million, with only 3% of Australian businesses having a turnover of more than $5 million.[19] We expect needs of the community will also further increase, noting the OAIC received 497 notifiable data breach reports in the six months from June to December 2022, up 26% from the prior reporting period.[20] And since the APPs were introduced in 2014, PI collection, storage and use has grown significantly, with the technologies used to collect, store and analyse this information advancing in complexity and sophistication.

Reforms of the Act's enforcement regime should be designed to promote certainty and clarity, and be targeted for maximum impact from a compliance perspective. For this to be achieved, the following factors should be considered:

- A clearly articulated and flexible enforcement regime that allows the regulator to act with enforcement tools which reflect the complexity of the Act and penalise non-compliance;
- Adequate OAIC funding, providing the resources necessary to pursue penalties under the enforcement regime in order to create appropriate disincentive;
- Consideration of a third-party certification regime as an additional measure to instil confidence that a base level of privacy compliance exists across APP entities;
- Appropriately considered rights for individuals to take action under the Act; and
- A robust data breach notification regime that reflects the reality of data breaches and minimises administrative burden for APP entities in the midst of an incident.

As outlined above, initial reforms to the Act should be targeted at 'low hanging fruit', focussed on areas that will have maximum impact with minimal added complexity.

Criminal and civil penalties

We agree more consultation should be performed with regards to introducing a criminal offence provision under recommendation 4.7. Consultation should be focussed on the anticipated utility of this new criminal offence, considering the extent of re-identification and exploitation of the PI of individuals in our community (for instance, the act of re-identification in the current cyber threat ecosystem may be less likely given the proliferation of PI following major data breaches). We do make note of existing criminal law offences that already apply to capture the proposed 'harm' or gaining of the 'illegitimate benefit', such as obtaining financial advantage by deception and blackmail.

The application of such a criminal offence provision should also be considered. In the context of the extra-territorial nature of many cyber threats and state-sponsored attacks, this criminal provision may be difficult to enforce in practice. Further, the proposed offence appears to contain a number of elements that would need to be established in order for it to be applied, and each element adds complexity and the ability for an accused to establish reasonable doubt. Finally, clarity will be needed on the exceptions that would apply, and the specific situations in which malicious re-identification of de-identified information would be permissible.

PwC generally supports the reforms to the civil penalty regime under the Act as proposed in Proposal 25.1 to establish a more targeted and flexible enforcement regime. Further, PwC generally agrees with Proposal 25.2 to clarify the existing civil penalty provision, however PwC urges removal of new ambiguous concepts such as 'information of a sensitive nature'. PwC's view is that recommendation 25.4 should only be considered where appropriate mechanisms are introduced to free up the resources of the regulator to participate in inquiries.

Additional funding and a multi-regulatory approach may increase the utilisation of the new regime. As a result and subject to the below, PwC generally supports the reforms to the civil penalty regime under the Act as proposed in Proposal 25.1. PwC's view is that this more targeted and flexible enforcement regime would be greatly beneficial for the OAIC and APP entities alike. Strict liability for minor breaches, such as privacy policy and collection statement deficiencies, should be considered in relation to large APP entities that have been subject to the Act for some time. A potential solution is the introduction of a 'straight through' approach to enforcement (within the proposed tiered model), where non-compliance is quickly detected and triggers a potential notice and fine. It will also be necessary for relevant regulatory bodies to actively exercise their powers and participate in this new scheme, otherwise the reform will have no practical impact.

[19] Counts of Australian Businesses, including Entries and Exits, July 2018 - June 2022
[20] Notifiable Data Breaches Report: July to December 2022 | OAIC

Any reforms to the enforcement regime need to be designed to increase certainty for the benefit of the regulator and regulated entities. Hence, we generally agree with the changes to section 13G in Proposal 25.2 to provide clarification for both organisations and OAIC. We largely agree with the suggested list of what the term 'serious' may encompass, and believe there is a sufficient balance between the flexibility and certainty of the proposed wording. However, we encourage the removal of ambiguous language in any amendments to ensure new concepts introduced are appropriately explained in guidance material or defined within the Act itself. For example, the concept of 'information of a sensitive nature' may create additional uncertainty to the already well established sensitive PI distinction.

The proposal to allow the OAIC to undertake public inquiries and reviews into matters under Proposal 25.4 would require additional resourcing of the OAIC. However, more thought needs to be given to the possible scope and nature of the type of inquiries proposed. There should be consultation and specification on what powers would be granted to the Information Commissioner in relation to such inquiries, which is something that would need to be addressed and clarified before inclusion of a regime of this nature.

In addition to the proposals made in the report, the government should consider the further tailoring of the civil penalty provisions to target particular non-compliances which have a significant flow on effect for the OAIC in enforcing the privacy regime. For example, the government may wish to consider a specific civil penalty provision relating to a failure by an APP Entity to notify the OAIC and affected individuals in relation to an eligible data breach (or at least deem a failure of this to be a serious interference with privacy). This would be justifiable on the basis that the failure to notify could leave individuals vulnerable to serious harm and without the ability to protect themselves, and also limits the OAIC's ability to take relevant regulatory action in relation to an incident.

OAIC funding model

PwC supports the investigation of appropriate funding models for the OAIC as set out in Proposals 25.7 and 25.8 and suggests the government go beyond Proposal 29.2 and consider the establishment of a multi-regulator regime (similar to the SOCI regime). This would serve to leverage the knowledge and resources of established industry-specific regulators.

As outlined above, the OAIC's task of regulating the current regime is significant and, with the proposed new powers and reforms to enhance the regime, this task would increase exponentially. Hence, PwC supports the investigation of appropriate funding models for the OAIC as set out in Proposals 25.7 and 25.8. Such funding should be multi-pronged in purpose, providing adequate resourcing for enforcement and compliance activities, as well as enhancing the OAIC's ability to undertake educational and guidance activities. Consideration could also be given to the establishment of a specialist enforcement arm within the OAIC.

Multi-regulator approach

In addition to investigating funding models for the OAIC itself, another complementary strategy would be to consider the role other sector-specific regulators could play in supporting the OAIC in enforcing and supervising the Act. For example, under the SOCI regime, a mechanism has been included to allow for certain industry-specific regulators to act as the specified Commonwealth regulator. Given Australia has many established industry-specific regulators - many of which are already, in their own way, attempting to regulate the use and protection of data by the organisations they regulate - there is an opportunity to leverage their knowledge and resources to provide additional support to the OAIC.

For this to occur, we submit that Proposal 29.2 could be expanded as it relates to regulatory cooperation, with the potential to implement a multi-regulator regime, similar to the SOCI model. Such a mechanism would help avoid duplication, provide consistency for organisations operating in specific sectors and allow for a more targeted approach to compliance and enforcement on an industry-specific basis. Furthermore, there could be scope to consider whether certain powers under the Act should be delegated to industry specific regulators.

We have further outlined the opportunity for regulator alignment in relation to data breaches and cyber security incidents below, which also goes to the outcomes of Proposal 29.2.

Another way of implementing a 'lighter touch' multi-regulator approach to the Act would be to go beyond the amendments proposed to the privacy code provisions of the Act in proposal 5.1. The government could consider making APP codes compulsory for certain industry sectors and have the supervisory regulator for that industry (for example APRA for financial services, AEMO for energy, ACMA for telecommunications and media etc.) responsible for consulting on, drafting, supervising and enforcing their codes in relation to relevant APP entities. This would have the benefit of allowing specialist industry regulators to apply the principle-based APPs to their industry sectors in more binding specificity, whilst leveraging their already established supervisory and enforcement functions to support compliance. The OAIC would be able to take a higher level coordination role in relation to these codes, working with the relevant industry regulator to ensure appropriate governance and oversight.

Third-party certification regime

PwC suggests the government consider an appropriate third-party certification regime. An appropriate combination of mechanisms will need to be utilised to mitigate risks of organisations that choose to opt for non-compliance. Given the scale of the task, even with an expansion of the OAIC's resources, it may be difficult to meaningfully engage APP entities, especially if the Act is expanded to all small businesses.

While additional rights of action for individuals and the introduction of a tort for serious invasion of privacy would assist in raising the risk profile of privacy issues across the economy, consideration should be given as to whether such legal routes would be meaningfully accessible to 'average' citizens, given the cost of litigation in Australia. This is particularly pertinent at the small business level where, in the event of a breach, there would likely be a more limited number of impacted individuals, with legal action not financially viable.

There may be value in exploring the viability of a third-party certification regime to support the application of key minimum protections under the Act. The government should monitor approaches and learn from experiences in other global jurisdictions. Having this as an additional mechanism would provide the OAIC with a level of confidence that a minimum level of compliance was being met across the economy, especially at the small business level (if the small business exemption is removed). This would ultimately assist the OAIC to concentrate its efforts and enforcement activity on larger organisations holding higher volumes of PI and organisations holding more sensitive information. Further, to incentivise small businesses to uplift their privacy protections, a subsidised third-party certification program could be considered.

Direct right of action for individuals

PwC supports a mechanism to enable individuals to personally take action for relief where there has been a certain level of interference with their privacy, as per Proposal 26.1. However, consideration should be given as to what standard should apply to the individual right of action when there is an expansion of civil penalties for lesser breaches.

Generally, we are in support of establishing an avenue for individuals to to personally take action for relief where there has been a certain level of interference with their privacy as per Proposal 26.1. That being said, the design and implementation of such a mechanism must be carefully considered. An unintended consequence may be that, introducing a direct right of action, there may be a shift of enforcement responsibilities to the courts. The question also remains as to what standard should apply to the individual right of action when there is an expansion of civil penalties for lesser breaches.

A robust notifiable data breach regime

We support Proposal 28.1 to reduce duplicate notifications and administrative burden for APP entities in the midst of breach incidents. The Notifiable Data Breach (NDB) Scheme is a lynchpin in the privacy enforcement regime. While not all failures to comply with the Act result in NDBs and not all data breaches arise from failures to comply with the Act, this scheme has forced organisations to engage with the regulator and to protect individuals whose information has been compromised.

Organisations with similar but slightly differing notification obligations for a number of regulators, under a number of regimes, are being required to make numerous notifications in the event of a breach. For example, some APRA-regulated entities have to make notifications under the Act, prudential standard and SOCI notification obligations. In our experience, this duplication causes significant administrative burden when an organisation is in the midst of an incident.

As a result of multiple regimes operating across different jurisdictions and sectors, there are varying levels of breaches that require notification, unnecessary duplication of notifications, and differences in timing and information needs. Harmonisation of notifiable requirements would increase efficiency and simplify notification, both for entities and governments. Thought will also need to be given on how to manage the different details that need to be shared with different regulators, how data may be shared among regulatory bodies and whether there are data breach notifications under the CDR requiring alignment. The adoption of a central repository for NDBs and cyber incidents (of some sorts), can enable the elimination of duplicate notifications and remove administrative burden in the event of an incident.

PwC supports aligning the NDB scheme with GDPR requirements and the suggested change of timeline to 72 hours for notification as set out in proposal 28.2. This will need to address situations where there is insufficient information to determine if the data breach is eligible for notification. A 'lesser trigger' for regulator notification may be relevant in this situation, such as the regulator being notified if there is a likelihood of material harm or chance of serious harm. This would support the OAIC's assertion that lack of evidence of data extraction is not sufficient to conclude an eligible data breach has not occurred,[21] noting investigations into these types of incidents are often extremely complex. Threat actors deliberately cover their tracks within systems and even claims data has been exfiltrated can be false. In this situation, a 'lesser trigger' notification consideration would be of value, providing notice to the regulator while giving an impacted entity time to further investigate an incident to gain a better picture of its severity.

[21] Playing dumb no longer an option against ransomware reporting

We support appropriate “practices, procedures and systems” to enable organisations to respond to a data breach, and suggest more guidance be shared to define these concepts, providing greater clarity for organisations so adherence is not unrealistic or difficult. Further, this should align with requirements under other pieces of similar legislation to ensure it can be leveraged to avoid duplication and inconsistency.

With regard to this Proposal 28.3, there is utility in ensuring that as much information is made available to affected individuals as is possible to enable them to take actions to protect themselves. In our experience, many organisations already do this for their own commercial interests, especially to protect their reputation with stakeholders. However, this proposal will result in additional obligations that need to be adhered to during the incident response.

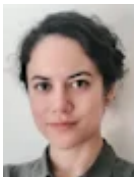
We agree that enabling the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach under Proposal 28.4 would be greatly beneficial for the public. Allowing the sharing of information when appropriate to prevent further exploitation of PI is a system that has been proven to work and be effective. However, there should be limits as to the amount of data allowed to be shared with appropriate safeguards to prevent abuses of power.

Contacts

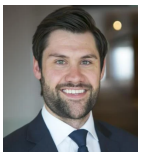
Jon Benson
Partner, Cyber Security & Digital Trust
jon.benson@pwc.com

Adrian Chotar
Partner, Legal
adrian.chotar@au.pwc.com

Natalie Mu
Director, Cyber Security & Digital Trust
natalie.mu@pwc.com



Victoria Young
Director, Cyber Security and Digital Trust
victoria.young@pwc.com



James Patto
Director, Legal
james.patto@au.pwc.com

Anne-Louise Brown
Chief of Staff, Federal Government Cybersecurity and Digital Trust
anne-louise.brown@pwc.com