Contribute to the conversation

Review of the Privacy Act 1988 (Cth)

KPMG Australia
Submission to the Attorney-General's Department Issues Paper

January 2021

KPMG.com.au

As a leading professional services firm, **KPMG Australia (KPMG)** is committed to meeting the requirements of all our stakeholders – not only the organisations we audit and advise, but also employees, Governments, regulators and the wider community.

Contents

Executive Summary

KPMG Australia (KPMG) welcomes the opportunity to provide a submission to the Attorney-General Department's review of the Privacy Act 1988 (Cth) (the Review). The Review is a significant opportunity to contribute to an important reform process that has the potential to empower consumers and protect their data, while creating economy wide benefits.

As a leading professional services firm, KPMG is committed to meeting the requirements of all our stakeholders – not only the organisations we audit and advise, but also employees, Governments, regulators and the wider community. We strive to contribute to debate that seeks to develop a strong and prosperous economy and society and welcome the opportunity to provide a submission to the Review.

The Review is an important and timely opportunity to once again reflect on our national approach to the regulation of data privacy. The Privacy Act recently marked its 30-year anniversary. While the Act has seen considerable reforms in that time (notably the introduction of the Australian Privacy Principles and Comprehensive Credit Reporting in 2014, and the Notifiable Data Breach scheme in 2018), it is important to ensure that Australia continues to have a privacy framework that achieves the right balance of protecting individuals and enabling entities to effectively respond to the challenges and harness the benefits of a free flowing data driven digital economy and society, in a balanced and proportionate way and provide certainty and guidance.

The terms of reference for the Review, and the questions posed in the Issues Paper, raise a broad range of matters that would have wide-ranging impacts on government, business and consumers.

As noted in the Issues Paper, substantial consideration has been given to many of these matters in previous reviews. KPMG's submission is therefore not intended to respond specifically to every question raised, but to draw on our multi-disciplinary subject matter experts across the firm to provide feedback on some key themes and issues which we believe should be considered in planning for this reform process.

Our comments centre on the following broad key themes raised in the Issues Paper:

- The reform process
- Objectives of the Privacy Act
- Definition of personal information
- Exemptions to the Privacy Act
- Notice of collection of personal information
- Consent to collection and use and disclosure of personal information
- Control and security of personal information
- Overseas data flows and third party certification
- Enforcement powers under the Privacy Act and role of the OAIC
- Consumer data rights
- Interaction between the Act and other regulatory schemes

As a technology neutral and principles-based law that prescribes individual information privacy rights and corresponding obligations, the Privacy Act provides flexibility for organisations to develop and implement a risk-based approach to the protection of personal information they collect and process. However, as the Issues Paper identified, there are a number of complex questions that are important to reflect upon to ensure that the right balance continues to be struck for a clear, streamlined framework that meets the needs of government and business and the rights of individuals in an evolving digital society and economy.

The Australian Information Commissioner Angeline Falk has flagged four key elements of reform that she considers are needed to support effective privacy regulation over the next decade:

- Global interoperability: making sure our laws continue to connect around the world, so our data is protected wherever it flows.
- Enabling privacy self-management: this enables individuals to exercise meaningful choice and control.
- Organisational accountability: to ensure there are sufficient obligations built into the system.
- A contemporary approach to regulation: having the right tools to regulate in line with community expectations.

There are two critical questions to consider, given the significant and potentially wide-ranging nature of the reform. First, what the key objectives of the Review are, in addition to addressing the consumer privacy rights issues identified by the Australian Competition and Consumer Commission (ACCC) in relation to digital platforms, and second, what is the most effective approach to reform.

Entities currently must manage and comply with a range of regulatory requirements that exist in overlapping and in some cases fragmented data-related frameworks at both a State and Federal level. New data frameworks are currently being developed. Given the nature of data flows and the convergence of data-related rights, data security standards and regulatory frameworks and standards both in Australia and globally, it will be important to take the opportunity to carefully consider how the Privacy Act interacts with these frameworks and provides a robust and clear national framework.

Central to this is how reform will help provide Australia with a comprehensive framework that maintains or strengthens key data protection principles, standardises and clarifies obligations, ensures the rights of individuals and the free flow of information and communication are protected, while minimising the imposition of further regulatory burdens to achieve a net benefit for all participants.

Lastly, the Review must also consider the impact of COVID-19 on how we work and interact with businesses and government in what will be a new normal. Digitisation of government and citizen centric services and the increasing use of digital contact tracing and QR codes, where citizens provide more information to connect and verify their identity, are becoming increasingly critical and the data protection framework needs to support this.

KPMG looks forward to continued engagement as this important review process progresses.

Regards,

Mark Tims
Partner

Head of Technology Risk & Cyber Security
KPMG Australia

Kate Marshall
Partner

Head of KPMG Law
KPMG Australia

Overview of key themes:

1. The reform process

The Issues Paper raises questions that open the way for potential wide-ranging reforms of the Privacy Act. Clarity about the objectives of the reform and how these will be achieved should be a primary consideration of the Review. This could be clearly articulated by committing to undertake a Regulatory Impact Statement to assess costs and benefits of reform options.

The Review must also consider the increased digitisation of government and citizen centric services accelerated by COVID-19 and the use of digital contact tracing and QR codes. The data protection framework will need to be resilient and reflective of how we work in a new normal.

2. Objectives of the Privacy Act

The key features that underpin the regulatory framework, as a principles-based and technology neutral law, are still appropriate. Some prescription may be helpful. But clearly defined concepts and rules, supported by the regulatory tools of code-making, guidance and advice, should be preferred as the most effective means for enabling compliance.

It is an appropriate time to revisit the fundamental privacy protections and principles that are embedded in the regulatory framework and assess whether these are effectively supporting the Act's objectives in a digital age, as well as whether they need updating or further articulation or clarification to ensure individuals are protected and entities know how to comply. This should have regard to developments in data protection regulation elsewhere and embed the principles of privacy and security by design and by default, accountability, data minimisation and transparency, data quality and integrity, consumer choice and control.

3. Definition of personal information

The Privacy Act regulates personal information. The definition determines the breadth of what data is regulated. Any changes should be carefully considered. The current definition provides sufficient flexibility to cover technological developments. Over-prescription should be avoided, and further guidance can assist. Consideration should also be given to how the Privacy Act can effectively regulate digitally driven biometric data and templates.

4. Exemptions to the Privacy Act

In addition to the definition of personal information, any changes to the small business and employee records exemptions will have the most significant impact in terms of expanding the regulatory framework to more organisations and imposing additional regulation. Removing these exemptions will help bring the Privacy Act into alignment with the GDPR. The purpose of their removal and whether this happens in whole or in part and the economic impact this would have, requires careful consideration and an assessment of how any changes will interact with other aspects of the current regulatory framework and any amendments.

5. Notice of collection of personal information

We agree that notice is a fundamental privacy tool and done well can be very effective. It has a separate function to a privacy policy. It supports the principles of transparency, accountability and enhances trust. The Review should assess how to make notice more effective in practice in a way that strikes the right balance to avoid notification fatigue, drives timely and meaningful notification, while maintaining flexibility. The adoption of well-designed notification processes and use of accepted icons in certain circumstances should be considered.

6. Consent to collection and use and disclosure of personal information

Consent has become increasingly relied on as a basis for the lawful collection, use and disclosure of personal information. The effective use of consent as a default legitimate basis for collecting and processing personal information should be reviewed in the context of the development of information technology, the use of data surveillance, cloud computing and increasingly data driven business and government.

While improvements to the notice and consent model are in principle welcome, the approach the ACCC has advocated in its Digital Platforms Inquiry may not be fit for purpose for the acts and practices of all types of entities that must comply with the Privacy Act. Obtaining meaningful and lawful consent in relation to all types of personal information and all practices in relation to it, is not always possible or practical and places the onus on individuals. The Review should also investigate alternatives to consent as a means for lawfully processing personal information, such as legitimate interests, in a manner that does not compromise privacy protections.

7. Control and security of personal information

Privacy and security are two separate concepts with specific rules that both support the protection of individuals' privacy and the principle of accountability. In addition to the principle of privacy by design, we also support the Review considering how the principle of security by design can be introduced and embedded in the APP framework.

We consider that the Notifiable Data Breach Scheme has helped to lift privacy awareness and to advocate for the need to take privacy, data security and training seriously. However, we consider there remains a need to encourage entities to focus on improving technical controls to support breach prevention which would further benefit entities and individuals.

8. Overseas data flows and third-party certification

There remains uncertainty about the application of the concepts of use and disclosure in the data transfer setting, particularly as the digitisation of data and development of technology and cloud computing change and increase the ways in which data is interacted with. We suggest that the Review considers the options and benefits of adopting standardised language to provide further clarify and consistency. Australia does not provide any certainty through an equivalency mechanism or process that recognises the adequacy of overseas privacy laws that are similar to the European Commission's adequacy decision-making process for GDPR.

The question of whether Australia should seek adequacy to the GDPR will depend on the approach to reforming other parts of the Privacy Act, such as the small business and employee exemptions. These exemptions have been identified as the main reason why the Privacy Act is not considered to be adequate by the European Commission. The Review should examine whether the absence of adequacy has proved to be a barrier to data flows and the impacts on business and consumers.

9. Enforcement powers under the Privacy Act and role of the OAIC

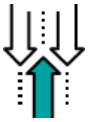
The availability and use of a range of regulatory tools that are appropriate to the circumstances and allow flexibility is in our view the most effective approach.

We are seeing a convergence of regulators step into the privacy framework particularly following the DPI Inquiry. The impact of this is yet to be determined, but we see a potential risk of additional burden on entities that must respond to multiple regulators on essentially similar matters, which also risks confusing consumers, and this overlap should be carefully considered as part of the Review.

10. Consumer data rights

The adoption and use of the concept of alternative applicable legal bases for processing personal information, such as consent or legitimate interest, would in our view help to enhance the interests of individuals in the management and control of their personal information and balance the burden imposed by the reliance on consent.

KPMG considers that the introduction of a new right to erasure of personal information or to a right of direct action or a statutory cause of action in the context of the Review needs to be carefully considered. Other rules, mechanisms and processes can effectively incentivise compliance and help achieve meaningful outcomes for individuals.



11. Interaction between the Act and other regulatory schemes

The adoption and use of the concept of alternative applicable legal bases for processing personal information, such as consent or legitimate interest, would in our view help to enhance the interests of individuals in the management and control of their personal information and balance the burden imposed by the reliance on consent.

KPMG considers that the introduction of a new right to erasure of personal information or to a right of direct action or a statutory cause of action in the context of the Review needs to be carefully considered. Other rules, mechanisms and processes can effectively incentivise compliance and help achieve meaningful outcomes for individuals.

Key themes considered

1. The reform process

Context and drivers for reform

The Privacy Act underwent major reform in 2014 (with the introduction of the APPs and the comprehensive credit reporting) and again in 2018 (with the introduction of the NDB Scheme). Since then, the role of technology and data in the economy and in society has continued to change and increase, at an accelerating pace.

The law is always being challenged to keep up with technology. The Privacy Act has broadly been able to effectively respond. A number of factors make the Review important and timely and require us to think about what the purpose, process and outcomes of reform should be:

- the impact of the global COVID-19 pandemic accelerating digital transformation and the collection of personal information for contact tracing and dissolving boundaries of data, society and enterprise
- the learnings from the DPI Inquiry
- the rise and ever-present threat of cyber-attacks
- use of artificial intelligence (AI)
- a connected global data supply chain
- the expansion of big data
- the role of ethics and trust
- importantly, community expectations.

Privacy and consumer rights are converging. New cyber, digital and data laws are being developed. The increased digitisation of government and citizen centric services due to COVID-19 and the use of digital contact tracing and QR codes are important reminders that the data protection framework will need to be resilient and reflective of how we work in a new normal. The APS Privacy Code is a good example of an enforceable working code in practice.

It is in this complex and dynamic environment that the Review must proceed. Therefore, clarity of the purpose of reform and how the process will happen is paramount. For example, if the objective is to achieve adequacy for GDPR purposes then some significant changes will need to be made. However, this should not be the driver. The development of a regulatory framework that is responsive to the rights of individuals and needs of entities in the Australian context should in our view be the primary objective. This could be clearly articulated by committing to undertake a Regulatory Impact Statement to assess costs and benefits of reform options.

2. Objectives of the Privacy Act

Privacy Act objects

The expansive list of objects outlined in section 2A of the Act have, in our view, endured well since they were introduced 20 years ago.

In particular, the object "to recognise the protection of the privacy of individuals is balanced with the interest of entities in carrying out their functions or activities" is fundamental to the Privacy Act framework, reflecting the need to strike a balance between consumer protection and information privacy rights and the legitimate interests of organisations in conducting their business, driving growth and innovation, which underpins a thriving economy that benefits all society.

Privacy Act framework

KPMG broadly supports the principles-based and technology neutral approach of the Privacy Act, supported by regulatory guidance. This regulatory approach to regulating data provides flexibility that is important given the wide variety of contexts in which the Act applies, and the speed at which organisations' practices and technologies they employ or use may change.

However, we believe that the Review is an opportunity to ensure that the framework is sufficiently flexible and provides the clarity needed in relation to some aspects of the regulatory framework and to consider how the regulatory and privacy tools can be best utilised and applied.

This relates to the connected supply chain and cloud computing, the related issues of accountability for notification of collection and processing and data security, as well as the lawful bases on which personal information can be processed.

The application of certain Australian Privacy Principles (APPs) to cloud services, for example, is not always clear.[1]

Further articulation of, and guidance on, the key underlying data protection principles that have broad application would in our view enhance the effectiveness of the framework while maintaining flexibility. These principles could include privacy and security by design and by default, accountability, data minimisation and transparency, data quality and integrity and consumer choice and control.

There continues to be misunderstanding or confusion about the meaning of key privacy concepts. Some of the terminology used in the Privacy Act and guidance and the definitions has contributed to this. The Privacy Act does not distinguish between a data controller or processor and their obligations and accountability and the meaning of the 'acts and practices' of entities in relation to data is not always understood. Further consultation and review of terminology would be welcome.

[1] A plausible reading of APPs 3 and 5 would require a service provider to provide a collection notice to individuals who deal with the provider's customers, despite the provider having no direct relationship with the individuals. Although Chapter 5 of the APP Guidelines outlines situations in which it may be reasonable to take no action to notify individuals under APP 5. We suggest, however, that legislative clarity is preferable to non-binding guidance.

3. Definition of personal information

Defining personal information

The definition of personal information is the foundation or trigger on which the operative provisions of the Act rely – both the obligations that must be complied with and the protections afforded to individuals.

KPMG supports preserving rather than amending the current definition and suggests instead that the existing guidance and APP Code-making powers in the Act could be better utilised to provide more clarity about what is personal information and address industry-specific concerns and specific privacy risks that may require specific protections.

Any significant change to the definition would have a fundamental impact on APP entities, requiring them to undertake considerable review of their entire privacy frameworks, systems and processes, including Privacy Impact Assessments (PIAs). The current definition reflects the original intent of the Privacy Act to be technology-neutral, principles-based and outcome-focussed rather than prescriptive. Any amendments should therefore be made only based on clear evidence of increased benefits or reduced impacts, having regard to the objects of the Act.

There are several specific aspects of the definition of 'personal information' that, in our view, should be clarified to provide certainty under the Act.

Technical Information

Expanding the definition to include 'technical information' runs the risk of embedding a static assessment based on today's concepts of technical data, rather than enabling a dynamic assessment. Including metadata or "data about data" may blur the line between where an individual's information ends, and an APP entity's proprietary information starts.

De-identified, anonymised, and pseudonymised information

Clarity about the concepts of 'de-identified', 'anonymised' and 'pseudonymised' information may be better protected or governed under industry-specific codes and should be the subject of further guidance which also allows flexibility to evolve. Any attempt to enshrine in legislation an industry-accepted technical standard of de-identification or anonymisation should be resisted. Industry may not itself agree on the standard and it would be inconsistent with the technology-neutral objects of the Act. The arguments concerning encryption standards (as a result of the NDB Scheme amendments prescribing the protection of information by security standards as a matter relevant to serious harm), demonstrates the difficulty of reaching a consensus and the risks of prescribing technical standards which might be outdated as soon as they are inserted.

Further, defining precisely which standards of de-identification are acceptable could deter entities from attempting to de-identify data - in case they face harsh enforcement by regulators. This will undermine entities' incentives to process and share de-identified data that could be used to improve AI systems, while at the same time driving some to process personal data when de-identified data would suffice, and as a result incur unnecessary compliance costs and restrict their range of legal uses.

Biometric data

Biometric data is increasingly captured and used for a range of purposes in digital form by both agencies and entities, including facial recognition, and there are associated privacy risks. Several moratoria are currently in place in various jurisdictions in relation to facial recognition technology and the OAIC is currently conducting a joint investigation with the UK Information Commissioner[2] into the use of biometrics by a facial recognition technology developer. Consideration should be given to how the Act can and should effectively regulate digitally driven biometric data and templates.

[2] *https://www.oaic.gov.au/updates/news-and-media/oaic-and-uks-ico-open-joint-investigation-into-clearview-ai-inc/*

4. Exemptions to the Privacy Act

Small business exemption

Removing the exemption altogether would impose significant regulatory burden on many small businesses whose data practices are minimal or low risk.

The decision about if and to what extent the exemption should be removed should not depend on the objective of an adequacy finding by the European Commission. The issue should be considered in the Australian business and privacy context. However, if a sector is excluded from the Privacy Act, any adequacy finding on the legislation must also exclude the sector.

In practice, given the connected data supply chain, many small data driven businesses who provide services to APP entities will be required by these entities to agree to comply with the APPs thus extending compliance.

KPMG notes that the Act already prescribes carve outs for certain categories of small businesses whose data practices are a higher privacy risk. The Review should consider how effective this approach is and whether any further carve outs should be prescribed.

The number of employees is in our view an arbitrary threshold for data protection given that many small businesses can develop and operate powerful software and technology or process large amounts of data with very few employees.

The turnover threshold reflects a level of financial capacity of entities whose businesses do have a higher privacy impact to meet the regulatory burden.

Employee records exemption

We repeat our comments above about the approach to the purpose of amending or removing the exemption in any way.

The purpose of removing the employee records exemption needs to be examined closely to strike a balance between data protection for employees and placing greater burden on employers when collecting and handling their employees' personal information.

In practice the exemption has become relatively confined for a number of reasons:

- it has been interpreted narrowly by the courts (see for example *Jeremy Lee v Superior Wood* Pty Ltd [2019] FWCFB 2946 which found that collection practices are excluded from the exemption, although the OAIC has not updated its guidance in response)
- the requirement for employers to comply with surveillance and health records laws
- the exemption only applies to the employer entity and not to any service providers to which they outsource any human resourcing processes such as payroll
- the exemption does not extend to Tax File Numbers
- employers generally apply similar security protections to all their data including employee data
- employers are offering employees benefits to support health and well-being and social engagement, such as gym memberships, health services or wellbeing programs.

Should any changes be made to the exemption, the role of consent in an employee-employer relationship will need to be addressed and is specifically dealt with in the Issues Paper. This is because there is substantial doubt as to an employee's ability to freely provide their consent given the power imbalance in an employee-employer relationship.

This has been raised in the context of the GDPR in the guidelines on consent adopted by the European Data Protection Board[3], which suggest that an employee cannot freely provide their consent to their employer and therefore it is problematic for employers to process the personal data of their employees on the basis of consent.

Removing the exemption would also expose employers to employment related claims for interfering with employee privacy in the context of what is an already complex fair work regime. Further the obligation to process employee access and correction requests could result in a significant burden being imposed on employers. Any revision of the exemption should not add further complexity to the data-related compliance employers are currently managing and any cost should be considered as part of a Regulatory Impact Statement.

[3] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

5. Notice of collection of personal information

Improving awareness of relevant matters

Consistent with the objects of the Act, the current approach to collection in APPs 3 and 5 allows APP entities to balance the protection of the privacy of individuals with their own interests in carrying out their functions or activities and should remain unaltered. As an example of its effectiveness, the notice test in APP5.1 has allowed for evolution of notice over time from providing paper-based notice when the Privacy Act was introduced to digital notice on websites to now notice in the bottom of most email communications and part of agreeing to sign up for digital services. The ubiquity of this approach has meant that it is now easier for individuals to obtain the notice that they require, and there are now more opportunities to more closely scrutinise the notice provided to ensure that the purposes of collection, use and disclosure are clear and adhered to by the APP entity.

Third party collections

In considering how the current system responds to the concept of indirect collection, notice needs to remain practicable and that the current system correctly places the onus on the APP entity collecting the information (or on whose behalf the information is being collected) to properly inform the individual of any indirect collection or potential transfer of data to a third party. Broadening the requirements to provide notice across a data supply chain over and above that original notice would lead to a greater burden on individuals as well as notice fatigue, in receiving, reviewing, digesting and consenting to privacy notices.

Limiting information burden on individuals

Reflecting the ACCC's Digital Platforms Inquiry Report, we agree that there should now be a focus on limiting the information burden on individuals being made aware of matters relevant to helping them make informed decisions. The Review should consider how the form, content, timing and delivery of more standardised notices can be provided that enhance user experience and empower users to understand the privacy consequences of providing their personal information to obtain goods or services. These could include mandating the form of notices, requiring summaries of key notice elements, encouraging layering and requiring the use of standardised icons or phrases. There would need to be further consultation on the design and user experience of the notice process. Agencies such as Data61 could assist from their work on the Consumer Data Right.

6. Consent to collection and use and disclosure of personal information

Consent to collection and to use and disclosure of personal information

APP3 requires APP entities to define the scope of purposes for which they collect personal information and reflect this in their notices. Organisations must ensure that they benchmark these purposes against collection being 'reasonably necessary for, or related (or for agencies, directly related) to, one or more of their functions or activities'. APP entities can generally only use or disclose the personal information they collect if it is for that primary purpose for which it was collected (APP6.1).

APP entities must have consent to collect sensitive personal information, which rightly imposes a higher threshold for collection and therefore subsequent use and disclosure.

Consent is one basis that APP entities can rely on to use and disclose the personal information they collect for a secondary purpose. Given the nature of exemptions available in APP6, consent has become heavily relied on as a basis for the lawful use and disclosure of personal information for a secondary purpose.

A review of the role, elements and benchmark of consent as a lawful basis for processing personal information cannot occur without also considering the collection and the notice framework. Any amendments must ensure that the regulatory burden is not disproportionate, with a focus on effective and meaningful disclosure through notices at or before the time of collection to enable valid consent to be provided. Again, the work of agencies such as Data 61 would assist.

Direct marketing

Our view is that the continuation of the opt-out system in relation to consent for direct marketing is consumer-focussed and effectively allows individuals to choose the extent of their engagement with an APP entity consistent with the current Spam Act requirements. Whilst the use of direct marketing has pivoted to digital and at size and scale, the ability for consumers to simply un-subscribe or withdraw their consent to direct marketing at any point has generally not been inhibited. In practice, we understand APP entities rarely directly market without an understanding that the individual has either consented to be contacted or there is an awareness that their information is being used for this purpose. Due to the nature of brand and reputational damage when APP entities directly market without that consent or reasonable expectation, again, the current system balances the requirements of an APP entity to generate marketing contacts with its conduct within the marketplace.

Definition of personal information

As one of our overarching themes for reform (discussed above), we recommend that clarity and certainty be guiding principles of any reform of the Privacy Act, and this extends to the definition of personal information. The current definition of personal information is, in our view, sufficiently clear that inferred personal information is a form of personal information, and we do not see a clear need to amend the definition to expressly include inferred personal information.

However, we suggest that the Act could be amended to clarify whether specific obligations apply to inferred personal information, in particular, whether the act of inferring personal information amounts to a collection of personal information ('collection by generation'). In our view, the Act is insufficiently clear on this point. While there are occasional references to inferred personal information in the OAIC's guidance[4] the present review offers an opportunity for a clear policy and regulatory position to be taken on this issue.

The role of consent for IoT devices and emerging technologies

The continued development and uptake of IoT technology and solutions will have a significant impact and role to play across all sectors of the economy ranging from smart cities to healthcare, transport, retail and smart energy in the home. IoT relies on the collection and sharing of data from and between a range of internet connected devices and the use of the combined data to unlock insights, drive value, increase efficiencies and innovation that will benefit individuals, the community and society more broadly. This will depend on their delivery of safe, effective and trusted IoT, which includes ensuring the right privacy and security settings. These are not unique to IoT but to technology and systems more broadly.

Careful consideration therefore needs to be given to how the regulatory framework can enable this to happen. Embedding clear data protection principles including security by design and consumer choice and control will be important elements. The fragmented regulatory framework particularly in relation to surveillance, (addressed in section 11 below) also needs to be addressed.

As highlighted elsewhere in this submission, consent cannot be relied upon as the solution to these challenges. We suggest the Review consider the notices, the adoption of clear and common standardised language and terms as well as icons can be used to provide consumer choice and control.

[4] For example, Chapter B of the APP Guidelines states (para B.28) that 'Collection may also take place when an APP entity generates personal information from other data it holds, such as the generation of an audit log.'

7. Control and security of personal information

Managing security

As cyber security threats have evolved significantly over recent years, so too have the complexities in understanding and assessing the risks they pose to the personal information entities hold. In our view, further guidance and clarity on control areas or matters that entities must consider when assessing whether their security is reasonable and appropriate would help improve practices to protect personal information. Similar provisions have been made in other regulatory instruments such as the GDPR (Article 32), and the APRA CPS 234 Prudential Standard.

For example, the specific inclusion in the GDPR of an appropriate measure being "*a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*" should be considered.

Privacy and security are two separate concepts with specific rules that both support the protection of individuals' privacy and the principle of accountability. In addition to the principle of privacy by design, we also support the Review considering how the principle of security by design can be introduced and embedded in the APP framework. For example, by including requirements to assess security risks.

Data retention

In our view the requirements placed on entities to destroy or de-identify personal information are appropriate and balanced. The challenge entities face is the potentially conflicting requirements of other laws and regulations to maintain records as well as the timely and effective destruction of digital data given the way it is stored and backed up.

The impact of the Notifiable Data Breach (NDB) Scheme

In our view, entities' practices have changed since the commencement of the NDB Scheme, largely in the detection and response aspects of breach management. We have observed that enhancements to the prevention of breaches appears to be more focussed on education and awareness. We consider that the NDB Scheme has gone some way in lifting privacy awareness and helping to advocate the need to take privacy, data security and training seriously.

However, there has been less focus on improvement of technical controls to support breach prevention and protection as a direct consequence of the NDB Scheme which is an area we consider entities should be encouraged to also focus on.

An area where clarity would be welcome was demonstrated by the data breach of an online recruitment services organisation which impacted multiple Australian entities and resulted in confusion about which entity should be notifying, individuals were burdened with multiple breach notices and the privacy benefits of this were unclear.

8. Overseas data flows and third-party certification

The adoption of cloud computing and the increasingly connected global data supply chain means that trust in the effectiveness of the cross-border data framework is critical, for business, government, consumers and regulators.

APP8 cross-border scheme

The cross-border scheme in APP8.1 supported by the OAIC's APP guidance in our view is generally working well. It provides a flexible risk-based framework for entities to follow and appropriately incentivises them to maintain oversight and assure compliance through the accountability provisions. There remains uncertainty about the application of the concepts of use and disclosure in the data transfer setting, particularly as the digitisation of data and development of technology and cloud computing change and increase the ways in which data is interacted with. We suggest that the Review considers the options and benefits of adopting standardised language to provide further clarify and consistency.

The effectiveness of the APP8.2(a) and (b) exceptions do raise some challenges. In order to rely on these exceptions, an entity must undertake an assessment of the protections afforded by a jurisdiction in which the overseas recipient is located, and such an undertaking can be extremely burdensome on the entity (and potentially duplicates work done by similar entities). Australia does not provide any certainty through an equivalency mechanism or process that recognises the adequacy of overseas privacy laws that are similar to the European Commission's adequacy decision-making process for GDPR. This can result in an ad-hoc approach to reliance on the jurisdiction exception or it is otherwise considered as part of the APP8.1 assessment.

The requirements for obtaining for valid consent for the purposes of relying on APP8.2(b) means its application is potentially very limited save in some very specific cases, or the validity of the consent is uncertain.

We suggest that these APP8.2 exceptions and how they can effectively support cross-border transfers as part of the scheme should be included in the Review. In particular, an equivalency mechanism similar to the adequacy mechanism under GDPR would provide certainty and reduce burdens on business, without introducing any impact on individuals.[5]

Adequacy

The question of whether Australia should seek adequacy will depend on the review of APP8 and the approach to reforming other parts of the Privacy Act, such as the small business and employee exemptions. These exemptions have been identified as the main reason why the Privacy Act is not considered to be adequate by the European Commission (as noted in the Issues Paper). We note that data exchanges for law enforcement are subject to separate arrangements.

[5] This could be achieved under the Privacy Act through the inclusion of equivalent jurisdictions in the regulations or through a rule-making power, for example.

An adequacy decision would mean that entities can rely on the exception in APP8.2(a) for data transfers to recipients in the European Union. This would also provide further certainty for handling data flows from Europe. However, this should not be the only driver for the approach to reforming these exemptions. The Review should examine whether the absence of adequacy has proved to be a barrier to data flows and the impacts on business and consumers. Entities will still wish to obtain contractual assurances and rights in relation to the protection of personal information they transfer particularly where they effectively continue to be responsible and need to control the data.

There is on the other hand an increased focus on data sovereignty and a desire for entities and government to keep data stored onshore, particularly critical data.

CBPR

The APEC Cross-Border Privacy Rules (**CBPR**) has not yet been introduced. This system is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally recognised data privacy protections. The CBPR System implements the PEC Privacy Framework[6] endorsed by APEC Leaders in 2005 and updated in 2015. Any further take-up or endorsement of the CBPR should be carefully considered in the context of the overall objective and net benefits.

[6] https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf

9. Enforcement powers under the Privacy Act and role of the OAIC

Regulatory tools that are fit for purpose and support compliance

The OAIC uses a blend of tools to encourage compliance, investigate complaints and achieve conciliated outcomes where appropriate and which entities can actively participate in. The availability and use of a range of regulatory tools that are appropriate to the circumstances and allow flexibility is in our view the most effective approach.

We are seeing a convergence of regulators step into the privacy framework particularly following the DPI Inquiry. The impact of these is yet to be determined, but we see a potential risk of additional burden on entities that must respond to multiple regulators on essentially similar matters, as well as confusion for consumers, and this overlap should be carefully considered as part of the Review.

10. Consumer data rights

The role of consumer choice and control and the privacy tools that support this principle is an important one that the Review should consider further in the context of a digital economy.

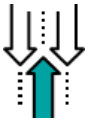
The adoption and use of the concept of alternative applicable legal bases for processing personal information, such as consent or legitimate interest (similar to Article 6 in the GDPR), would in our view help to enhance the interests of individuals in the management and control of their personal information and balance the burden imposed by the reliance on consent.

Statutory tort

The Review would need to give further careful consideration to inserting a direct right of action or a tort of privacy in the Privacy Act. In KPMG's view it would not be the most appropriate mechanism to include in the context of how the regulatory framework operates. The provision in section 13G of the Privacy Act and the powers and functions of the Information Commissioner enable the impacts of serious privacy breaches to be addressed. The remedies in the Privacy Act as well as other legislation and the common law in our view provide the appropriate balance.

Introducing a new right to erasure

The introduction of the 'right to erasure' in the GDPR was in a very different context to Australia. It is not apparent that there is a need to introduce a specific right. As the Issues Paper identified, the current data rights and regulatory powers of the Information Commissioner require (under APP 11.2) personal information to be deleted in appropriate circumstances. The impact of introducing such a right on a range of other interests, freedoms, rights and law enforcement activities would need to be carefully assessed and the perimeter of the right clearly defined, and consideration should be given to enhancing APP 11.2 through amendment or guidance, rather than introduction of an entirely new obligations.



11. Interaction between the Privacy Act and other regulatory schemes

Separate privacy protections for addressing specific privacy risks and concerns

KPMG recognises that some specific privacy risks and concerns may require specific protections. However, rather than the creation of additional, separate regulatory regimes, we suggest that it would be preferable to address such situations under the framework of the Privacy Act, including through the code-making powers in Part IIIB of the Act. This would assist in ensuring that any additional obligations or protections were consistent with the broader Privacy Act obligations and protections, reducing the risks of uncertainty and complexity for both regulated entities and individuals. This has been effectively done in relation to the COVIDSafe app framework.

The collection and use of biometric data through the global acceleration in the development and use of 'biometric technologies', in particular facial recognition technology (**FRT**) (comprising software, AI and other surveillance mechanisms) is a specific area that requires further consideration, given the privacy risks and impacts. The Australian Human Rights Commission released a discussion paper on the interaction between human rights and emerging technologies[7] which includes consideration of the privacy related issues. We refer to KPMG's March 2020 submission *Human Rights and Technology in 2020 and Beyond* for a more detailed assessment of the privacy implications of emerging technology[8].

Harmonisation of privacy protections under Commonwealth law – addressing fragmentation

Broadly, KPMG agrees that some (not necessarily all) of the Commonwealth laws offering privacy protections address particular issues that may be appropriately addressed in legislation other than the Privacy Act.

In some instances, however, the existence of multiple privacy regulatory schemes can create uncertainty or duplication. For example, the existence of direct marketing requirements in both APP 7 and the *Spam Act 2003* (Cth) may be seen as unnecessary given that the requirements of both schemes are broadly similar (e.g. the requirement of a functional opt-out mechanism).[9] Another example is the overlapping data breach notification regimes.

---

[7] *Australian Human Rights Commission ('AHRC'), 'Human Rights and Technology' (Discussion Paper, AHRC, December 2019)*

[8] *https://assets.kpmg/content/dam/kpmg/au/pdf/2020/human-rights-and-technology-2020-and-beyond-kpmg-submission.pdf*

[9] While APP 7 is focused on the use and disclosure of personal information for direct marketing purposes rather than on unsolicited commercial electronic messages *per se*, in practice the requirements are quite similar. The carve-out in APP 6.7 for direct marketing, coupled with the carve-out for the Spam Act in APP 7.8, in our view, adds to this unnecessary complexity.

We suggest that the Review give further detailed consideration to these matters, and we note that the response to certain other issues in the Issues Paper may be relevant considerations (for example, any amendments to the definition of personal information that would capture communications data may be relevant to the harmonisation of the Privacy Act with telecommunications privacy protections).

A major challenge for compliance and effective data protection continues to be the overlapping and fragmented surveillance and health records laws which are largely State and Territory based. These create dual and often conflicting regimes for entities to comply with and can be confusing for consumers to understand and to engage with. They have been the subject of piecemeal amendments which has led to greater fragmentation. It means multiple regulators can potentially deal with the same issue or complaint. This also results in a lack of common and clear privacy-related terminology and guidance to apply, for example in relation to the definition and use of surveillance in the context of developing technology.

There are also separate Commonwealth statutes that have data breach and reporting frameworks which also overlap and are potentially inconsistent with the NDB Scheme. Finally, we note the current development of additional data frameworks and data rights regimes. It will be important to ensure that these are as consistent as possible and do not create the challenges that are noted above. The Privacy Act should remain the foundational national privacy framework around which such legislation is developed.

Broadly, **KPMG agrees** that some (not necessarily all) of the Commonwealth laws offering privacy protections address particular issues that may be appropriately addressed in legislation other than the Privacy Act.

Key authors and contacts

Veronica Scott
Director, Legal
E: vscott1@kpmg.com.au
T: +61 3 8667 5711

John Jordan
Senior Compliance Analyst, Business Services
E: jjordan3@kpmg.com.au
T: +61 3 8663 8127

Angela Dally
Associate Director, Privacy
E: adally1@kpmg.com.au
T: +61 3 9288 5333

Kath Slack
Associate Director, Privacy
E: kslack1@kpmg.com.au
T: +61 3 9288 5235

Matthew Quick
Director, Management Consulting
E: mquick@kpmg.com.au
T: +61 3 9288 6015

Joe Green
Manager, Management Consulting
E: jgreen15@kpmg.com.au
T: +61 3 8663 8094

Steven Robertson
Associate Director,
Audit, Assurance & Risk Consulting
E: srobertson8@kpmg.com.au
T: +61 2 9335 8914

Sophie Finemore
Associate Director, Regulatory Affairs
E: sfinemore@kpmg.com.au
T: +61 3 9288 6226

Shubham Singhal
Associate Director,
Audit, Assurance & Risk Consulting
E: ssinghal4@kpmg.com.au
T: +61 3 9288 5401

KPMG.com.au