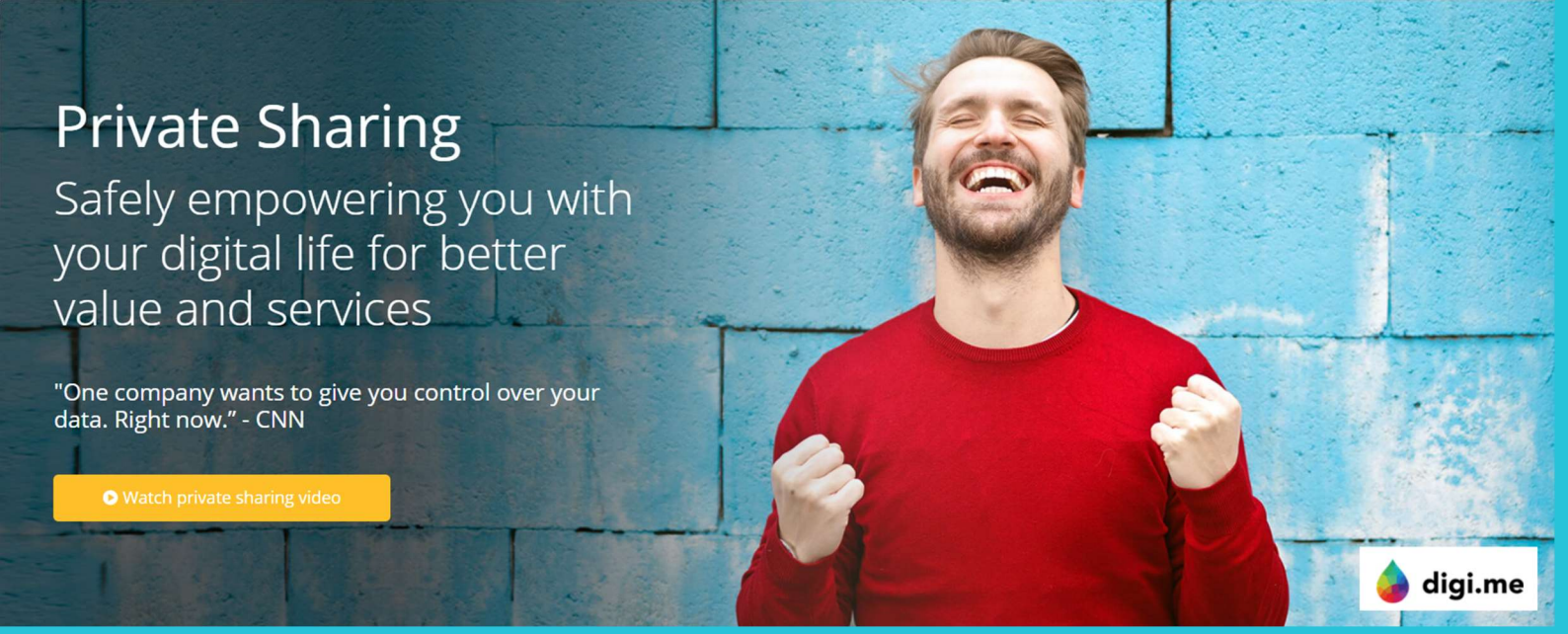


Australian Privacy Act Review

Submission for the Attorney General's Department

Author |Joanne Cooper
ID EXCHANGE IN PARTNERSHIP WITH DIGI.ME
4TH DECEMBER 2020

Disclaimer – the views expressed in this submission have been provided in good faith and are based on our own beliefs and industry knowledge which is subject to change without notice due to the rapid evolution of the Data Economy, legislation, and world events. E.&.O. E

ID Exchange Pty Limited
Stone & Chalk FinTech Incubator
Wynyard Green
11 York Street
Sydney NSW 2000 Australia

www.idexchange.me

Privacy Act Review | Integrity and Security Division
Integrity and International Group
Attorney-General's Department
Submission emailed to | PrivacyActReview@ag.gov.au

December 4th, 2020

Privacy Act Review – Response to Issues Paper

Australian Data Exchange, the overarching brand of ID Exchange, provides the Australian market with a range of enabling, consumer-centric, personal data sharing exchange platforms.

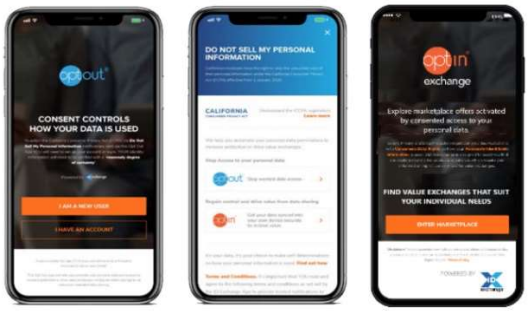
As an industry stakeholder, ID Exchange in partnership with digi.me welcomes the opportunity to comment on the Issues Paper for the review into the *Privacy Act 1988* (Cth) (Privacy Act), in particular, whether the scope of the Privacy Act and its enforcement mechanisms remain fit for purpose.

This submission complements previous submissions made by ID Exchange in relation to the Productivity Commission's Data Availability and Use report, the Consumer Data Right Act and the Data Availability and Transparency Bill.

About ID Exchange

ID Exchange is a Sydney based, Australian company that was established in 2012. We develop privacy enhancing technologies (PETs) and digital rights management solutions to assist consumers to protect and mobilise their data for their benefit. Our technologies provide consumers with the means to control and manage their data using methods such as unified opt in and opt out consent controls. Further information about ID Exchange can be found at https://idexchange.me.

Sample of ID Exchange consumer facing consent activation apps automating data access legislation.



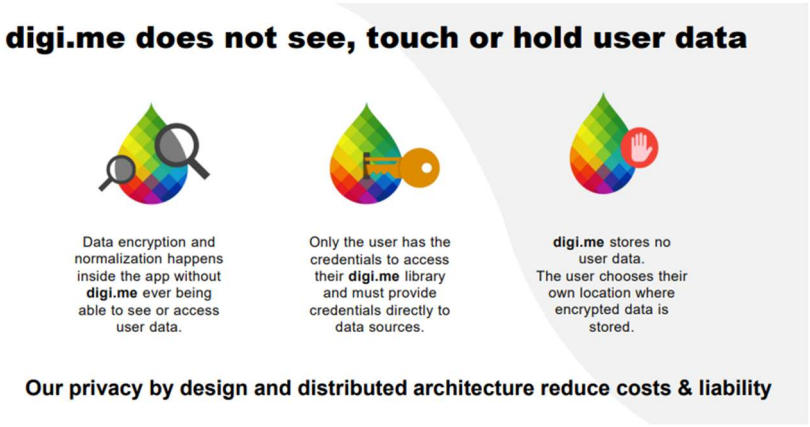
ID Exchange in partnership with digi.me is committed to the adoption of ethical consent management and related security frameworks that provide an interoperable and consumer-centric approach to personal data sharing in a digital environment. ID Exchange is happy to discuss any of the issues covered in our submission in further detail upon request.

About digi.me

digi.me is a platform that enables individuals to securely aggregate, view and exchange their personal information from multiple sources and, with their consent, to decide how it may be shared with others.

Digi.me:

- provides individuals with the means by which they can connect, access and keep their personal information up to date in real time from multiple different data sources
- links to multiple data sources via Apps, web-based services and other structured and unstructured databases through Application Programming Interfaces (APIs)
- enables people to securely download their personal information and to store it in a device or other cloud storage location of their choosing, with the entire process safeguarded using strong encryption
- enables individuals to understand better the nature, extent and value of their personal information through a dashboard that provides both a visual representation of it as well as curating it so that people can 'make sense' of their own data holdings
- provides individuals with functionality that enables them to share their personal information safely if they choose to do so on the terms that they determine



In short, it is a privacy preserving technology (PPT) that gives people awareness of, and control over, their personal information.

Digi.me uses a decentralised architecture to implement this process. This means that at no time does digi.me touch, hold or see its users' data. The digi.me platform does not sell or trade user data. It does not tell its users how or where to share their data. The platform provides the data pipes between individuals and the holder of their data and those to whom they wish to share their data in a way that is private and secure.

As a private and secure data exchange platform, digi.me enables data portability; complies with the requirements of the European Union's (EU's) *General Data Protection Regulation* (GDPR) and has been subject to an EU data protection impact assessment (DPIA). To satisfy EU and other international privacy requirements, it adopts a 'Privacy by Design' approach to protecting personal information. digi.me also meets or exceeds international security standards.

digi.me's functionalities are flexible and scalable. They are not limited to any particular categories or to industry or social sectors. Currently, they include health, finance, social, wearables and entertainment.

Overview of Current Privacy Environment

Alongside members of the MyData Global forum, and a multiplicity of other organisations providing PPTs or privacy enhancing technologies (PETs), ID Exchange and digi.me recognise that individuals' views on privacy may vary widely, depending upon the presence or absence of trust, their degree of knowledge about privacy issues and risks, their ability to protect their privacy (technical 'know how'), and whether or not they obtain a benefit or advantage from disclosing their information.

In short, there is no one-size-fits-all approach to privacy, with individuals changing their views over time, between organisations, and in accordance with their preferences or personal beliefs. This spectrum of views produces demand for a range of technical solutions, including new or enhanced ways of managing consent.

Currently, it is difficult for individuals to have a clear view of the way in which their information is collected, used, disclosed, stored and otherwise handled despite the fact that privacy legislation is pervasive and technical solutions exist for a range of privacy issues and risks. Currently, there is a limit to any individual's ability to manage all relevant privacy issues and risks on their own. We believe that it is important not to underestimate the number of people who would like to adopt more privacy-aware data practices but do not have the knowledge or technical ability to do so. Privacy regulators, backed by appropriate legislative frameworks, can help individuals take steps to protect themselves and develop greater trust in the online environment.

Increasing concerns around transparency and fairness, as well as a renewed interest in ethics, are a direct response to increasing complexity, monetisation and opacity in the personal information ecosystem. We are seeing regulators around the world questioning whether or not the approach to personal data taken by large digital platforms is lawful and fair. We are seeing governments around the world taking another look at their privacy legislation, asking whether or not it remains fit-for-purpose and making changes in

response. In addition to the EU, this has included the UK, Brazil, New Zealand, Singapore, California, and Canada. Previously 'dormant' legal policy issues – such as online tracking, surveillance and dark patterns – have become dominant.

Almost continuous data breaches, as well as the impact of the GDPR and Californian privacy legislation, have also contributed to a commercial shift away from the non-transparent collection and handling of personal information, towards more consumer-centric approaches. Multiple market responses are emerging to address these concerns. Whether this involves established players like Google changing their practices or Apple mandating pro-privacy requirements – or newer, 'privacy first' companies like digi.me developing innovative platforms, products and services – significant change is underway.

This activity demonstrates that PPTs and PETs are continuing to develop and evolve in response to privacy-intrusive products and services. In the mid-1990s, Privacy by Design, along with its 7 Foundational Principles, emerged in response to PETs' inability to gain traction. Almost 25 years later, in 2020, PPTs and PETs are no longer untested or failing to gain traction – they provide a component of an overarching privacy solution, alongside legislation, regulation, organisational practices and Privacy by Design or privacy engineering approaches. Any updates to the Privacy Act should be informed by these developments while maintaining the current principles-based and technology neutral approach.

Summary of Key Points

- We support the Privacy Act Review and welcome any changes or enhancements to the Privacy Act that enable it to remain up-to-date and meaningful, capable of tackling the specific privacy issues and risks facing us today
- We note the importance of the Privacy Act and the Australian Privacy Principles (APPs) remaining technology neutral. In particular, privacy legislation:
    - should not impede the development of multiple technical solutions, reflecting the multiplicity of individual views on privacy; and
    - should not prevent businesses from offering PPTs/PETs as part of, or the primary component of, their commercial offerings
- The Privacy Act should maximise consistency in its operation, including through the removal of unnecessary exemptions that result in increased uncertainty for individuals and organisations
- Recognising that consistency remains key to streamlining international privacy compliance requirements, Australia should continue working towards a global standard of privacy protection, thereby enabling a small technology business in Australia to operate on the same platform as other, larger businesses. Likewise, it is important that Australian companies provide Australian citizens with equivalent protection to EU citizens – this point, rather than 'adequacy', should provide the policy basis for pursuing consistency
- There is a need to separate out issues relating to 'consent' within the APPs, 'consent' within an entity's Terms and Conditions, and what may prove to be the 'death

throes' of consent-based cookies and related tracking technologies. Each of these involves different legal, regulatory and policy issues. They should not be conflated. A failure to separate out the various definitional, policy and legal/regulatory issues relating to consent is likely to result in further confusion and, potentially, lead to reforms that prove to be undesirable in the medium-to-long term

- Claims around 'consent fatigue' are overstated and avoid tackling the real issues faced by individuals. This aspect of the issues paper requires further, detailed contextual analysis. We note that numerous technical, regulatory and operational options are available now and can be used by entities and individual consumers to streamline consent processes. The key focus here should be protecting the individual's autonomy
- There are two core elements from the GDPR that should be considered as part of the Privacy Act reform process.
    1. A straightforward right to data portability that is consumer-centric and enables all entities to participate subject to meeting a minimum set of technical requirements (ensuring data portability is viewed first and foremost as an individual right)
    2. Explicit and informed consent (supplemented by the regulator as/if required) to ensure that individuals are protected from online tracking, surveillance and dark patterns (amongst other current issues)

Response to Specific Topics and Questions

The remainder of our submission provides responses to specific issues identified and questions raised in the Issues Paper.

Objects of the Act

First, simple changes to the wording of section 2A (a) of the Privacy Act could produce a positive shift in meaning. See, for example, a more action-oriented object (a), below.

> The objects of this Act are:
>
> a) to ~~promote the~~ protect~~ion of~~ the privacy of individuals; and
> b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities; and …

Second, in relation to subsection (b) (above), it is unsurprising that the ACCC expressed concern with the current wording, which, in 2020, appears *un*balanced. We think this is because the original source of this object – OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines), first published in 1980 – is no longer apparent. The OECD Guidelines were intended to help 'harmonise national privacy legislation and, while upholding such human rights, at the same time prevent interruptions in international flows of data'. To achieve this, the Guidelines sought to balance two

competing *public interests* – one involving the protection of privacy (human rights), the other promoting the free flow of information (economy).

The current wording of object (b) in the Privacy Act refers to the need to balance the protection of the privacy of individuals with the *interests* of *entities* in carrying out their functions or activities. Looking back to the original context of this object (the OECD Guidelines), it is clear that the balance sought is not between the individual and the entity *per se*, but between the public interest in protecting an individual's right to privacy protection vis-à-vis the use of their personal information as a key component of a global, digital economy (i.e., the free flow of data).

While the world has changed since 1980, the tension between the protection of privacy and the promotion of the free flow of information remains steady. We agree with a review of section 2A of the Privacy Act to ensure that its objects remain fit for purpose and that they remain aligned with the OECD Guidelines. If this approach is taken, it is unlikely that object (b) will remain in its current form.

Scope and Application of the Privacy Act

Definition of personal information

We note that the current definition in the Privacy Act was intended to operate expansively. A focus upon 'identifiability' (rather than 'identity', *per se*) was intended to enable a broader range of information to be covered by the definition. For many stakeholders, this idea of aggregate or cumulative identifiability made – and continues to make – sense, particularly in a digital world.

To the degree that the Full Federal Court in *Privacy Commissioner v Telstra Corporation Ltd* (the Grubb case) found a flaw in the drafting of the definition of personal information (i.e. 'about' an individual' is a threshold requirement to any consideration of identifiability), this should be addressed as part of the Privacy Act Review.

It is a moot point whether or not location data and other 'technical' data would have been considered 'identifiable' in the absence of this threshold requirement. However, based on the confusion the decision has caused – for a number of lawyers as well as commentators and the difficulties it has posed for the OAIC – we think it is feasible and desirable to update the definition of personal information.

This could include information 'relating to' rather than being 'about' an identified individual or an individual who is reasonably identifiable, as well as the inclusion of a *non-exclusive* list of elements that may comprise identifiability, including one or more examples of 'technical' data (e.g. location data, or an online identifier). We do not support inclusion of the term 'technical data' in its own right. We agree that the definition of 'personal data' found in the GDPR (see below) could be adapted to meet Australian drafting requirements.

> 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an

> online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In addition to confirming that technical data may contribute to identifiability, this would have the added benefit of harmonisation with the EU Directive.

Inferred personal information

Inferred or derived personal information is part and parcel of the digital world. Starting with the basic premise that personal information is protected under the Privacy Act, it is clear that inferred or derived personal information likewise should be protected if it meets the definition of personal information (as updated following the Privacy Act Review). This is similar to the scenario in which social media platforms prevent social media platform data being used by third parties for 'surveillance' purposes (largely through Terms and Conditions).

The *outcome* of the processing – personal information – not the process itself, should remain the focus.

It is also possible that there is a policy shortcoming in relation to Australia's current approach 'de-identification', which has exacerbated issues around inferred personal information (see below).

De-identified, anonymous and pseudonymous information

We argue that a major blind spot exists in relation to APP 2 (Anonymity), which must be considered *prior to* any discussion of de-identified, anonymous and pseudonymous information.

For many years it has been assumed that it is not practicable to provide individuals with the option of not identifying themselves, either because technical solutions did not exist, or because 'identity' was required. However, in 2020 there are a wide range of PPTs and PETs available that would enable APP 2 to have greater meaning in individuals' everyday lives. Interpretation of 'practicable' should now require recognition of a range of alternative approaches, including those enabled by technology. Further, as shown by digi.me, it is possible to provide individuals with a secure, decentralised platform through which they can control their own information without platform operator, seeing, touching or holding their data.

We consider that APP 2 should be given broader consideration by all APP entities but especially agencies, for whom APP 2 may mean 'anonymity first'. This is an area where further guidance is required from the OAIC in order to ensure that the scope of the Privacy Act remains fit for purpose.

In relation to 'de-identified, anonymous and pseudonymous information', a recent shift towards defining 'de-identified' – partly in response to issues caused by the re-identification of an Australian Government open data set – may not be aligned with the issues otherwise raised for discussion in this section of the Issues Paper. This requires further detailed analysis to ensure that the underlying legal policy issues have been identified correctly. A failure to review the approach to 'de-identification' may prevent appropriate action being

taken in relation to 're-identification'. In order to ensure the best outcome, a full analysis is required.

Additionally, if the current approach is retained we believe that suitable experts, including those with cryptographic expertise, be invited to review the security of Australian Government open datasets, prior to their publication. If the approach is updated, it would be beneficial for the terms 'identifying', 're-identifiable' and 'non-identifiable' (or equivalent terminology) to be re-inserted into the NHMRC Guidelines.

Flexibility of the APPs in regulating and protecting privacy

The APPs should continue to be at the heart of the Privacy Act. Overall, a principles-based, technology neutral approach provides the best legislative framework for privacy protection. allowing for some flexibility in practice. It is also consistent with international practice.

However, principles-based legislation is a complex form of regulation, producing a number of paradoxes – including a potential lack of certainty – that need to be taken into account in any law reform process.[1] In other words, there are reasons why stakeholders may view the APPs as opaque, uncertain, difficult to understand, etc. These views should not be taken as given, but looked at in context.

Further, and as noted directly below, the removal of exemptions from the Privacy Act, in particular, the small business exemption, will enable the APPs to be scalable to all entities, removing the need for 'special treatment' of entities considered to pose a higher risk to privacy but not covered otherwise by the Privacy Act.

As an aside, currently, the APPs provide a *minimum* standard. As a Code of Practice cannot introduce requirements that are contrary to or inconsistent with the APPs, it is unlikely that this mechanism will justify the effort required to develop a code for most organisations.

Exemptions

Consistency and certainty are key to reducing compliance efforts – both within Australia and internationally. Minimising exemptions will help to streamline the Privacy Act, reducing complexity as well as the compliance burden that comes with it.

Small Business

In order to provide a consistent and more certain privacy law environment, the current exemption for small business should be removed altogether. The benefits of privacy law coverage for digital businesses of any size outweigh any compliance burden, enabling them to compete on a global stage and ensuring that they are aware of key privacy issues and risks. The OAIC should be funded to develop a range of information sheets, tools and techniques specifically for small business to help reduce the regulatory burden, particularly for small businesses that collect, use and disclose minimal amounts of personal information. This could include support for automated privacy policy development where simple information flows are involved.

[1] Julia Black, 'Forms and paradoxes of principles-based regulation' *Capital Markets Law Journal* (2008) Vol. 3, No. 4: 425-457. For example, while principles can facilitate communication, they can also hinder it in practice, including through uncertainty.

Removal of the small business exemption will also obviate the need for entity-specific coverage of small businesses (such as residential tenancy database operators) or specific types of information (such as health information).

Employee Records

The exemption for employee records should be removed. It is not logical, fails to protect an individual's personal information end-to-end, introduces complexity/inconsistency in information handling, and does not deliver any clear public policy benefit.

Political Acts and Practices

The exemption for political acts and practices should be removed or tightened considerably to ensure that individual citizens are aware of the ways in which their information is currently being collected and used by political parties, including without their consent. Ensuring that Australia's system of representative democracy remains strong should not require citizens to give up the privacy of their personal information. It is fair that political parties should adhere to the same principles and practices required of the wider community.

Journalism

The exemption for journalism should be retained but reviewed to ensure that it remains fit for purpose.

Protections

Improving awareness of relevant matters and limiting information burden

The Privacy Act authorises or permits the collection and handling of personal information where it is required for an entity to perform its functions and activities. There is no requirement for consent in this situation unless the collection involves sensitive information, including health information. In this context – where consent is not a threshold requirement – it is not unreasonable to require collectors to provide notice, particularly in relation to more opaque aspects of a specific collection process.

At the same time, it is important not to place too much emphasis upon notice as a solution to information asymmetry. Notice occupies a more modest role. However, used well, it has the capacity to provide individuals with good quality information. Many of the problems associated with notice arise because of the complexity of information flows rather than the service or product offered.

There is a link between privacy policy and notice requirements that could be leveraged better to provide individuals with the information they need *before* their information is required (privacy policy) and/or at the point their information is required/collected (notice). Layered notices work well in tandem with a suitable privacy policy. Clarifying how these may be used 'cumulatively' may provide practice assistance to entities on the one hand and a counterbalance to overly legalistic notices on the other.

Limiting information burden (information overload)

We agree that the role of notice could be enhanced significantly through the development of iconographic or 'nutritional' labelling schemes. While icons have not become a standard component of privacy management/practice yet, there is increasing interest in such schemes' ability to reduce 'information overload'. While, up until now, the expected benefits that should accrue to a 'good operator' have not resulted in take up, the growing community awareness of a broad range of privacy issues and risks (and discomfort with their handling) and a general shift towards more privacy-respecting data practices by organisations suggest this may soon change.

Early icons developed by Aza Raskin for Mozilla in 2011 remain useful, and there are numerous examples of contemporary icon (EU terminology) or nutritional labelling (US terminology) work going on around the world.[2]

This work could be leveraged within Australia. Support for internationally consistent icons could be progressed through the forum of the Global Privacy Assembly and does not need to be backed by certification, at least in the short term. Any dishonest (misleading or deceptive) use of icons would be covered by the Australian Consumer Law, thereby acting as a disincentive to an Australian organisation doing the wrong thing.

Consent to collection, use and disclosure of personal information

This section of the Issues Paper opens with a problematic statement:

> The key way individuals exercise control over their personal information is through granting consent for entities to collect, use and disclose their personal information for different purposes. (p.41)

As outlined above, under the Privacy Act the collection of personal information is not based upon consent. There is no requirement under the APPs for individuals to consent to the collection of their personal information unless it is sensitive information, including health information.

This type of statement confuses or elides the difference between consent in relation to the APPs and consent under Terms and Conditions. It also overstates the role of consent within the Privacy Act. It is important to ensure clarity here as otherwise there is potential for misunderstandings to emerge and grow that will only become more difficult to resolve in the future if left unchecked.

It may be preferable to think about these issues in terms of autonomy, before turning to consent as one mechanism whereby individuals can exercise autonomy.

Pro-consumer defaults

We support pro-consumer defaults ('Privacy by Default'). These have the capacity to help individual consumers exercise their privacy choices more easily and effectively as well as

[2] See Aza Raskin et al, 'Privacy Icons': https://wiki.mozilla.org/Privacy_Icons; Appropriate Privacy Icons: https://privacypatterns.org/patterns/Appropriate-Privacy-Icons. In November 2020, Apple announced plans for easy to understand 'nutritional labels' to accompany its requirement that developers provide App information disclosure (effectively executing a form of icon privacy collection notices).

opening up the market to organisations that may operate on a 'privacy first' or 'privacy by default' basis.

Control and security of personal information

Security and retention

Information security remains a curiously underdeveloped aspect of the online world when one considers that it is the key to ensuring that personal information is collected and handled in accordance with individuals' expectations not to mention the significant amounts of money that government has spent on awareness raising. While it is not necessarily a component of legislative reform, it is suggested that the OAIC work with ASD and other relevant government agencies to ensure that practical, actionable recommendations and resources are available for users as well as small businesses.

Enhanced requirements to destroy or permanently de-identify personal information (as appropriate) would help reduce the degree of privacy risk associated with holding personal information in the first place.

Right to erasure

This aspect of the GDPR is subject to significant misunderstanding. Any discussion of a right to erasure as part of the Privacy Act Review process should proceed with caution, based upon accurate information. The right to erasure enables consent to be withdrawn in a technical context. This is necessary in order to provide genuine, consumer-centric data portability.

If this is not understood fully, there is a real risk that the role of the 'right to erasure' will be dismissed on the basis that it is not practicable. We urge the review process to seek to understand fully the relationship between consent, control and erasure ('right to be forgotten') in order to minimise the risk of misunderstandings arising. A shared understanding of terms and definitions is required.

Overseas data flows

Greater consistency in legislative schemes internationally will produce the best outcomes for Australian citizens and businesses. Choosing between the EU/GDPR and the APEC Privacy Framework – as is suggested in the Privacy Act Review Issues Paper – is a false dichotomy.

Regulation and enforcement

In order to administer the Privacy Act properly, the OAIC needs sufficient resources to execute current responsibilities as well as any new responsibilities arising from the Privacy Act Review. Sufficient funding enables regulators to do their jobs efficiently and independently.

Notifiable Data Breaches Scheme – impact and effectiveness

It is arguable that the ACCC's investigation into online health booking platform HealthEngine for misleading and deceptive conduct in relation to its collection and use of consumers' personal information, and the subsequent finding by the Federal Court that HealthEngine

had engaged in misleading or deceptive conduct in contravention of section 18 of the Australian Consumer Law, has had a greater impact than the Privacy Act's NDB Scheme.

The fact that HealthEngine was ordered to pay $2.9 million also contributed to the view that, under the Australian Consumer Law, the ACCC has the capacity to cut through misleading or deceptive privacy policies, 'name and shame' the organisation responsible, and impose suitably significant fines. Providing the OAIC with the capacity to issue significant fines will not necessarily change this situation in the absence of a 'name and shame' component. This requires consideration of whether or not the Privacy Act should remain primarily an educational scheme.

Interaction between the Privacy Act and other regulatory schemes

[Too much splintering between regulatory schemes is not good for privacy. It would be preferable for one agency to have primary responsibility for privacy. However, as long as the OAIC is focused upon education, prevention, promotion, soft touch, etc. it is unlikely to evolve into a regulator with muscles in the short term.]

Australian privacy laws have long been committed to a non-adversarial, educational approach to the regulation of privacy. This has had positive results over a long period of time. Further, if the small business exemption is removed from the Privacy Act, it would be preferable for small businesses to feel that they would not be 'sent to jail' on their first 'offence' (privacy breach). If the primary focus of the OAIC is education, then the ACCC should become the primary place for consideration of poor privacy practice that falls within the scope of the Australian Consumer Law. However, with the Australian Government's intention to increase the fines available to the OAIC, there may be an intention to change the regulatory model supported by the Privacy Act.

Overall, we remain convinced that Australia holds a key opportunity for well-considered Privacy reform which can harness and promote Australia's digital transformation position to enhance our data economy by leveraging the Regtech sector to ensure consumer centric technologies are utilised within the Privacy Act review.

As Privacy and Data Sharing platform leaders, please feel free to contact us for any further clarification or continued input in relation to this submission.

We look forward to continued participation.

Kind regards,

Joanne Cooper

Founder, Managing Director

ID Exchange Pty. Ltd.