Submission of Data Synergies in Response to *Privacy Act Review: Issues Paper*

Peter G Leonard

December 2020

DATA SYNERGIES

Contents

Submission of Data Synergies in Response to Privacy Act Review: Issues Paper

Peter Leonard[1]

Thank you for this opportunity to make a submission in relation to the Attorney-General Department's review of the Privacy Act 1988.

We have no objection to the publication of this submission.

We first make a number of general observations, and then address certain of your questions.

1 This review should endeavour to make Australian data privacy regulation fit for the next decade

The central problems with the Privacy Act 1988 are not as to coverage or comprehensiveness of the Act.

There are deficiencies in the current Act, including lack of clear statement of purpose and certain exemptions.

This review should address these deficiencies.

However, addressing these deficiencies alone will not render data privacy regulation fit for the next decade.

The central problems in practical operation today of the Privacy Act are:

(a) Lack of understanding of many APP entities (both businesses and government agencies) as to why, how and when to assess risks of privacy harm impacts upon affected individuals.

In particular, the Privacy Act is not at all clear as to when privacy harms that impact individuals are of a nature or magnitude that an act or practice should not be countenanced, regardless of notice to, or consent of, affected individuals.

[1] Peter Leonard is a data and AI business consultant and lawyer advising businesses and government agencies. Peter is principal of Data Synergies and a Professor of Practice at UNSW Business School (Management, and IT Systems and Management). Peter chairs the IoT Alliance Australia's Data workstream, the Law Society of New South Wales' Privacy and Data Committee and the Australian Computer Society's Artificial Intelligence and Ethics Technical Committee. He serves on a number of corporate and advisory boards, including the statutory NSW Information and Privacy Advisory Committee, which provides ongoing strategic advice to NSW Government as to data privacy. The views expressed in this submission are those of the author, not of other bodies and organisations, or clients of Data Synergies.

Fixing this problem requires much clearer guardrails in the Act, including:

- *The Privacy Act should expressly address the key concepts of privacy risks and privacy harms*.
- *There should be certain 'no-go zones', either statutory or by declaration by the Commissioner (following proper public consultative processes), including of behavioural advertising knowingly directed at younger children.*
- *There should be a requirement of (objective) reasonableness (appropriate purpose) in acts and practices of APP entities in collection, handling and disclosure of personal information about individuals.*

(b) Many APP entities do not have ongoing data privacy management programmes.

Privacy risk management by many APP entities is episodic, often associated only with commissioning of new projects and major changes that are subject to formal change management process.

Privacy impact assessments (**PIAs**) often are not conducted when they should be. PIAs often are conducted only when regulatory compliance people are called in, and not built into an APP entity's business processes and practices. PIAs often not revisited when an APP entity's everyday processes or practices in handling of personal information relevantly change.

Fixing this problem requires *obliging APP entities to implement practical, ongoing, operational data privacy management programmes (not only to conduct PIAs for projects of high impact)*.

(c) PIAs are often conducted as an audit style function, with the primary objective being reducing business risks of an APP entity, and not mitigation of privacy impacts upon affected individuals.

Compliance culture of many organisations (both businesses and government agencies) in relation to data privacy is poor.

Many organisations do not empower privacy officers to participate in key decisions about design and specification of products and services, and instead seek address privacy compliance as a documentation function.

A common exception from this shortcoming is governance of information security. This exception illustrates the broader problem. In recent years most businesses and government agencies have significantly improved governance of information security, largely due to recognition that serious data breaches are likely to lead to loss of enterprise value, erosion of trust of persons that deal with the APP entity suffering a breach, and exposure to class actions and ransom claims. Exposure to regulatory

penalties for serious data breaches may have been a factor in improving information security governance, but it is not the primary factor. Outside of management of information security, good data privacy practice has to date generally not been seen as a significant driver of enterprise value. As a result, many APP entities have a poor track record of implementation of data minimisation and data privacy by design and default, and in considering legitimate expectations of individuals in and to data privacy.

Fixing this problem requires rebalancing of incentives, regulatory requirements and sanctions to ensure that data privacy concerns that are not related to data exfiltration are accorded similar attention within APP entities to the attention now given to governance of information security.

(d) The primary, and often exclusive, data privacy focus of APP entities is upon two things:

- mitigation of legal compliance risk and reputational risk; and
- ensuring just enough transparency to meet requirements for notice and consent and comply with provisions of Australian Consumer Law.

Impacts upon individuals of excessive collections, uses and disclosures of personal information have not been properly evaluated and addressed by many APP entities.

As the Privacy Act is silent as to when, why or how APP entities should assess privacy impacts upon individuals, it should not be surprising that APP entities focus upon formal compliance, and not privacy impacts. The Privacy Act is poorly structured and unclear as to its purpose in ensuring that privacy impacts upon individuals are properly mitigated by APP entities, and that APP entities properly manage and disclose residual risks to and impacts upon affected individuals (through operation of the notice and consent requirements).

Fixing this problem requires a fundamental restructure of at least the front end of the Privacy Act, coupled with simplification in statement of key requirements.

This restructure and restatement is now particularly important because data collection and handling is becoming more pervasive and intrusive and data privacy affecting acts and practices become common across a broad range of organisations.

This existing problem will also become more widespread if coverage of the Privacy Act is expanded to include SMEs. The current Privacy Act is not sufficiently clear in its intended operation to be ready for the Act to apply to SMEs. Applying the Act in its current form will impose a significant regulatory burden on many organisations. This burden could be substantially lessened if the Act is restructured and restated.

(e) The Office of the Australian Information Commissioner is underfunded and under resourced.

Increases in penalties will not change compliance culture, unless the OAIC is also resourced:

- to be more actively involved in education and instruction,
- to promote development of industry best practice,
- to identify and call out examples of good privacy practices,
- to investigating possible, less egregious breaches of the Privacy Act,
- to run important but risky court cases,
- conduct sector benchmarking analyses and promote development of sector, product or service specific standards and codes of practice, and
- to conduct the kind of wide ranging and open-ended policy and industry reviews that the ACCC is funded to undertake.

The right of individuals to data privacy has been accorded a lesser status than the right of consumers not to be misled. Each right is important. Individuals should be afforded protection of legitimate expectations of data privacy even when they are not consumers.

Fixing this problem requires *commitment by the Federal Government to fund and staff the OAIC so that the OAIC is able to properly do its job*.

It is unfair and unrealistic to expect the OAIC to be an active and effective regulator given its current funding and resourcing.

(f) The privacy self-management (notice and consent) framework is broken. However, it is not so broken that it can't be fixed. The fixes include:

- supplementation (with a reasonableness (appropriate purposes) requirement and no-go zones, as to which see above),
- tidy-ups of the APPs relating to notice and consent (see later in this submission), and
- new carve-downs and exceptions, so that notices and requests for consent are focussed upon what is really important or unusual.

There should be carefully crafted exceptions for legitimate interests (including reasonable business purposes)[2]*, including promotion of individual interests and*

[2] See for example Part 3 of the new First Schedule to the Personal Data Protection Act of 2012 (**PDPA**) of Singapore, as amended in November 2020 by the Personal Data Protection (Amendment) Act 2020 (gazetted 10 December 2020 and pending commencement), and the *Draft Advisory Guidelines On Key Provisions Of The Personal Data Protection (Amendment) Bill* issued 20 November 2020 by the Personal Data Protection

societal interests, would focus the notice and consent framework and reduce the information overload burden upon individuals.

2 Restructuring and refocussing the Privacy Act

Our Privacy Act needs more than a tidy-up refresh. Fiddling at the edges of the current Privacy Act, and increasing nominal penalties, will not reset behaviours of many APP entities.

Many recent data privacy statutes around the world are now much better suited for current and emerging data handling practices of businesses and government agencies than our Privacy Act.

APP entities, and individuals, need better, clearer, data privacy law.

By way of one recent exemplar, we commend the structure, clarity and simplicity of Bill C-11 as introduced into the House of Commons of Canada on 17 November 2020 (https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading).

Within the first 30 clauses, the Bill clearly states the key requirements of data privacy law.

The purpose of the statute is stated as:

> "to establish — in an era in which data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information — rules to govern the protection of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances": clause 5.

Commission (PDPC) of Singapore: https://www.pdpc.gov.sg/guidelines-and-consultation/2020/11/draft-advisory-guidelines-on-key-provisions-of-the-personal-data-protection-(amendment)-bill. The Singaporean legitimate interests exception "is intended to enable organisations to collect, use or disclose personal data in circumstances where it is in the legitimate interests of the organisation and the benefit to the public (or any section thereof) is greater than any adverse effect on the individual. This could include the purposes of detecting or preventing illegal activities (e.g. fraud and money laundering) or threats to physical safety and security, ensuring IT and network security; and preventing misuse of services. To rely on this exception to collect, use or disclose personal data, organisations must first: (i) assess any likely adverse effect to the individuals and implement measures to eliminate, reduce the likelihood of or mitigate identified adverse effect to the individual; (ii) determine that the benefit to the public (or any section thereof) outweighs any likely residual adverse effect to the individual; and (iii) disclose their reliance on legitimate interests to collect, use or disclose personal data. This exception must also not be used for sending direct marketing messages to individuals.": Public Consultation Paper issued by The Ministry of Communications and Information and The Personal Data Protection Commission, Draft Personal Data Protection (Amendment) Bill, 14 May 2020, page 12, clause 7.

Bill C-11 then states:

> "An organization is accountable for personal information that is under its control": clause 7(1).

The Bill makes it clear that organisations should not be able to duck accountability by inability of a regulator or complainant to identify a human who should be the responsible person within an organisation. Our submission is that organizational accountability without responsibility designated to a particular individual role is meaningless: penalties then readily become just other costs of an APP entity doing business, and ensuring or verifying compliance are someone else's responsibility. The Bill accordingly continues:

> "An organization must designate one or more individuals to be responsible for matters related to its obligations under this Act. It must provide the designated individual's business contact information to any person who requests it": clause 8.

The Bill then recognises that an organisation is unlikely to reliably and verifiably comply with the law unless it embeds good data privacy governance in everything that the organisation does, through a program of compliance. The Bill states:

> "(1) Every organization must implement a privacy management program that includes the organization's policies, practices and procedures put in place to fulfil its obligations under this Act, including policies, practices and procedures respecting:
>
> (a) the protection of personal information;
>
> (b) how requests for information and complaints are received and dealt with;
>
> (c) the training and information provided to the organization's staff respecting its policies, practices and procedures; and
>
> (d) the development of materials to explain the organization's policies and procedures put in place to fulfil its obligations under this Act.
>
> In developing its privacy management program, the organization must take into account the volume and sensitivity of the personal information under its control": clause 9.

Responsibility of an organisation in relation to its service providers is then addressed:

> "If an organization transfers personal information to a service provider, the organization must ensure, by contract or otherwise, that the service provider provides substantially the same protection of the personal information as that which the organization is required to provide under this Act.": clause 11.

The Bill then creates an overarching "appropriate purpose" requirement:

> "12(1) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.
>
> (2) The following factors must be taken into account in determining whether the purposes referred to in subsection (1) are appropriate:
>
> (a) the sensitivity of the personal information;
>
> (b) whether the purposes represent legitimate business needs of the organization;
>
> (c) the effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs;
>
> (d) whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and
>
> (e) whether the individual's loss of privacy is proportionate to the benefits in light of any measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual": clause 12.

Only then does the Bill address notice and consent. Among other matters, it provides for exceptions from requirements for consent in respect of clearly and simply expressed "individual's interest", "socially beneficial purpose", and a number of other exceptions, but generally only when coupled with deidentification management: see in particular clauses 29 and 39.

This submission does not assert that in this Bill, the Canadians have 'got it all right'. Our point is that, although the APPs appear to be simply stated, the APPs are misleading. There is no clear statement of the way in which they are intended to be applied by an APP entity to assess and mitigate risk of privacy harms to individuals and to manage and properly disclose residual risks and impacts. Indeed, you can read the Privacy Act end to end and after 327 pages still have little idea of why or how an APP entity should assess and mitigate risks of privacy harms to individuals and manage residual risks.

If Australian data privacy law is restructured and restated, APP entities would have less scope to perceive that they could 'paper their way to compliance', or use behavioural psychology to 'game' requirements as to notice and consent.

3 Back to basics in statutory drafting in order to ensure digital trust and citizen participation in digital communities and the digital economy

We will achieve little more than collective exhaustion and loss of digital trust of citizens if the outcome of this Review is expansion of the definition of "personal information" and dialling up of requirements for notices and requests for consent.

Notices and requests for consent will remain not an effective control or safeguard for reasonable data privacy of citizens in many contexts of handling of personal information, regardless of however those notices and requests may be simplified, layered, targeted, made 'just in time', made not misleading, and made plain English and 'transparent'.

We need to go back to basics. Privacy law is now an important element in the framework of digital trust required to enable citizens to work, play and otherwise participate in their communities (however they choose to define them), in Australian society, and in the global economy. Privacy law reform should:

- protect legitimate interests and rights of individuals in and to data privacy (regardless of whether those individuals consumer products or services of a relevant APP entity), and
- nurture digital trust of citizens, to the benefit of affected citizens and of broader communities and societal interests, but also
- reasonably accommodate the imperative for governments agencies and businesses to derive efficiencies of operation and provide citizens with benefits derived from data and technology driven innovation.

As with the Australian Government's government data sharing reforms, citizens and agencies need to be empowered to understand why and how reasonable and proportionate collections and handling of personal information about individuals can deliver efficiencies and benefits while not undermining their digital trust and their rights to and interests in data privacy.

Data privacy is not just a consumer protection issue. Among other reasons, the relevant collection and handling of data may or may not be associated with a consumer transaction. Rights and interests of citizens in relation to data about them need to be protected regardless of whether they are engaged in a consumer transaction. Protection of legitimate rights and interests of individuals in and to data privacy should not be principally addressed through consumer protection regulation.[3]

Regulation of data privacy generally, and specifically of collection, use and sharing of geolocating and other individuating data collected from use of smartphones, IoT devices, digital search and social media platforms, content platforms, product and service comparison and ecommerce sites, is essential to enable citizens to go about their lives with reasonable seclusion.

[3] See further Manwaring, Kayleen, 'Will Emerging Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation' (September 1, 2018). Competition and Consumer Law Journal (2018) Vol 26, Issue 2, pp 141-181; Manwaring, Kayleen, 'Emerging Information Technologies: Challenges for Consumers' (April 25, 2017), Oxford University Commonwealth Law Journal (2017) Vol. 17(2), available at SSRN https://ssrn.com/abstract=2958514

Reasonable seclusion is the right or interest of citizens to go about their private lives in both public spaces and in private spaces: in places where people elect to congregate, in workplaces, in places where citizens cannot avoid being observed in public (i.e. streets, public transport, parks, shopping precincts), as well as in places and in the course of activities where people believe that are not being observed recorded or tracked.

Once upon a time, individuals could exercise choice as to whether they valued data privacy. The Privacy Act empowered them with information that they could (should they wish) read to assist in exercising that choice. Notice and consent requirements as embodied in the Australian Privacy Principles made sense when individuals had a choice of whether to deal with an APP entity or not. Now, increasingly valuable electronic data about citizens is both an essential enabler and inevitable exhaust of our activities during the conduct of our everyday life. Google Maps, our public transport apps and our toll tags get us to where we will do whatever we do.

Many apps gather data what we do when we get there, including in private and at home.

Many places into which we now venture won't allow us in without a digital registration.

Digital data collected, used and shared in myriad ways that often citizens cannot comprehend, let alone control, is an enabler and a by-product of what we think, do or feel, where, when and with whom.

Digital data is often collected without the affected citizen even being aware, let alone with properly informed knowledge or affirmative consent.

Increasingly, that electronic data is being used to profile both identifiable and unidentifiable individuals:

- to individuate what is offered to a particular individual (i.e. real time online behavioural advertising) or segments of individuals (i.e. inclusion audiences for online digital advertising), when, where, at what price and on what terms, or
- to exclude particular segments of individuals (whether or not identifiable) from offers.

The challenges to data privacy need not be seen as an existential crisis. We are not now facing the last opportunity that we will have to prevent our lives becoming a pantechnicon or subject to universal surveillance. However, we should recognise that the outcome of this Review will materially affect the path, timing and extent of expansion in intrusive collection and use of personally identifying information about Australians by diverse Australian government agencies, businesses and other organisations. This Review should not be narrowed down to focus upon the activities of a few global digital platforms or providers of digital advertising services. Not should this Review be distracted by discussion as to appropriate framing of consumer protection law in Australia.

If we think of most individuating electronic data as an enabler and exhaust of everyday life, and not as product of voluntary action (as informed through notice or consent), our focus rightly shifts to what an APP entity collecting, using and sharing that data is doing, and how responsible they are in how they are in doing it.

This fundamental shift in focus is why data privacy regulators around the world are now addressing organisational accountability of data controllers.

Organisational accountability of APP entities requires an appropriate regulatory framework to ensure that APP entities properly evaluate and mitigate, and properly manage residual risks, of privacy risks and privacy harms that individuals may suffer, from acts and practices of APP entities and other entities within data ecosystems enabled or managed by those APP entities, in collecting, handling and disclosing of personal information about individuals, and non-identifying but individuating data about an individual that is used to effect an outcome that are reasonably likely to have significant and adverse effect upon an individual.

Properly is shorthand for reliably, objectively, implementing good governance processes, and in how an APP entity manages multi-party and multi-purpose data ecosystems that the APP entity enables or in which the APP entity operates.

Individuating data is shorthand for data which may be used by an APP entity, or someone else that it enables or permits to use that information, to differentiate how a particular individual is treated, regardless of whether that individual is personally identifiable. In other words, this data may be either personal information about an individual as today understood, or what is sometimes called identifying profiling data – data about actual or inferred characteristics, attributes, preferences or other characteristics of an unidentifiable individual that is in practical application able to be used to significantly differentiate how that individual is, or small cohorts of individuals are, treated, as compared to other individuals. Individuating data is distinguished from audience segments, such as those commonly used today for targeted digital advertising services (but not one-to-one targeting).

Individuated effects may be positive: beneficial to the affected individual (whether or not identifiable), and/or to society generally (i.e. the public health and safety benefit when persons in contact with COVID positive individuals are able to be traced and checked, regardless of who they might be).

Individuated data often enables better digital inclusion of citizens, more efficient delivery of digital and offline services and products (i.e. enter once for whole-of-government services), disintermediation in supply and distribution chains (leading to more efficient markets and better choice and lower prices for end users), ability for a user to make a better comparison and evaluation of alternative products, services and providers, lessens friction in switching between providers, and so on.

All these benefits can be assured through by appropriately targeted regulation, without prompting a burden of requiring citizens to climb a reading mountain of notices and requests for consent, or continuing to allow (for instance, because notice was given somewhere sometime, and the citizen ill-advisedly clicked *I agree* in order to get on with real life) unjustifiably excessive collection and sharing of data about citizens and unreasonable surveillance, tracking or snooping.

The notice and consent framework is not so broken as to make the task of making notice and consent work in circumstances to which notice and/or consent are suited a hopeless cause. Citizens should not be disempowered from self-management of personal information about them in contexts where it is realistic to expect them to read notices and exercise fully informed choice. There continues to be good policy justifications for:

- a notice and consent framework,
- for appropriately legislated exceptions and exemptions from requirements to provide notice as to collections and handling of personal information generally, and
- requirements to obtain fully informed consent in relation to a sub-set of that personal information that should be classified as higher risk or sensitive.

However, the consequence of a citizen electing to make a decision to not read the notices, or being unable (for instance, due to youth or age, disability or poor comprehension of the English language) to read or understand the notices, should not be that the citizen is left without regulatory protection.

There are many scenarios where individuals may suffer significant privacy harms through excessive or otherwise unreasonable collection and handling of personal information about them, in circumstances where an APP entity fully complies with the APPs but is not held to account for excessive or otherwise unreasonable acts or practices.

Expanding the definition of *personal information*, changing *about an individual* to *in relation to an individual*, or tweaking requirements for *notice* or *consent*, would not ensure that an APP entity is able to be held to account for excessive or otherwise unreasonable acts or practices as to personal information about individuals.

The Privacy Act needs to address scenarios where APP entities intentionally or through poor governance practices cause or allow to occur significant privacy harms through excessive or otherwise unreasonable acts or practices of collection and handling (including disclosure) of personal information about individuals, including where an APP entity may otherwise fully comply with the notice and consent requirements stated in the Australian Privacy Principles.

APP entities should be required to act reasonably to assess, mitigate and manage residual privacy risks (being privacy risks that remain after taking proper mitigation measures) of significant privacy harms to affected individuals.

The concepts of *privacy risks* and *privacy harms* have been extensively analysed, discussed and used by data privacy regulators in comparable jurisdictions. Creation of this (proposed) requirement would be Australia striking out into unfamiliar territory.

This (proposed) requirement should operate regardless of whether an APP entity is otherwise subject to 'the full raft' of notice and consent requirements as stated in the Australian Privacy Principles. For example, if a policy decision is taken by the Australian Parliament that small to medium business enterprises (SMEs) should not be required to comply with some of all of the Australian Privacy Principles, SMEs should nonetheless be required to comply with this (proposed) requirement.

This (proposed) requirement should be framed so that it addresses significant privacy harms to affected individuals that arise as a direct result of excessive or otherwise unreasonable acts or practices of collection and handling (including disclosure) of personal information about individuals, regardless of whether the significant privacy harm to an affected individual is immediately proximate to an excessive or otherwise unreasonable acts or practices in handling of personal information.

In other words, the requirements should address significant privacy harms to affected individuals that are individuated effects enabled by profiling and automated decision making even where there is no direct and proximate use of personal information about individuals in creating the individuated effect.

Use by APP entities of non-identifying code for audience segmentation for digital marketing, or for individual specific online behavioural advertising, might therefore be within the (proposed) requirement, although properly managed audience segmentation services might continue not to be outside notice and consent requirements of the Australian Privacy Principles. If audience segmentation uses of non-identifying codes relating to devices or humans (being information that, if not the subject of proper governance by the relevant APP entity, could become personal information about an (identifiable) individual) is properly controlled and safeguard through good governance, there should not be risk of significant privacy harm to any affected individual.

Our answers to your specific questions now follow.

4 Responses to specific questions asked in the Issues Paper

4.1 Objectives of the Privacy Act

1. *Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?*

We recommend a more fundamental restructuring and refocussing of the Privacy Act: see section 2 above of this submission.

In any event, our answer is: yes, the objects outlined in section 2A of the Act should be changed.

The purpose and objects stated in the Privacy Act are useful guides as to the intended operation of the Act. However, on the current state of the law and principles of Australian statutory interpretation, these statements of purpose and objects are unlikely to significantly affect legal interpretation of the operative provisions as to those listed circumstances in which an act or practice is an invasion of privacy of an individual.

The concept of "responsible and transparent handling" in paragraph (c) of section 2A is neither adequately explained nor connected back what should be the dual role of transparency:

- providing openness to affected individuals, and
- enabling verifiability (and therefore accountability) of a regulated entity's acts and practices.

New readers of the Privacy Act are often surprised that the statute does not define *privacy*, *privacy risk*, or the circumstances in which an act or practice is to be taken to cause a relevant *harm* to an individual. Most operative provisions in the Privacy Act use *privacy* as an adjective (occasionally an adverb) in a description of something else: privacy policy, Privacy Act, Australian Privacy Principle, privacy authorities and so on. Section 2A is one of the rare instances where privacy is used as a noun and concept in and of itself: however, section 2A is not an operative provision, and the concept is not further explained.

The Privacy Act does not state what *privacy* is, or how to assess *risk* of *harms* of impact on the privacy of individuals, or require any assessment of whether any impact is *reasonable* or unreasonable. Indeed, the Privacy Act 1988 does not generally use *risk* or *harm* (other than in relation to whether a data beach is notifiable) as operative concepts.

The Overview in Schedule 1 - Australian Privacy Principles states that Part 1 of the APPs (APP 1 and AAP 2) "sets out *principles that require APP entities to consider the privacy of personal information,* including ensuring that APP entities manage personal information in an open and transparent way". However, the APPs do not state how APP entities should determine

the circumstances in which rights or interests of individuals in and to privacy are affected, or how to evaluated the nature or extent of harm to those rights or interests, in application of the APPs.

This review of the Privacy Act 1988 should address these deficiencies.

The objects clause should include an object of ensuring that acts and practices of APP entities do not unreasonably interfere with the privacy of individuals.

This should be coupled with *an operative provision to the effect that APP entities should only collect, use, or disclose personal information about individuals to the extent and for purposes that a reasonable person would consider appropriate in the circumstances*.

The objects clause should also include *an object of promoting fair and responsible handling by APP entities of personal information about individuals, through implementation of reliable and effective data governance, privacy enhancing technologies and practices, and appropriate monitoring, oversight and review process and practices*.

We also suggest *a further objective is included of providing enforceable rights for individuals to seek redress for an interference with their privacy*, in addition to any complaints process.

4.2 Definition of personal information

2. *What approaches should be considered to ensure the Act protects an appropriate range of technical information?*

The Act as it stands today is technologically neutral as to personal information about individuals.

This was appropriate, and remains appropriate.

Any inclusion of particular 'technical information' is likely to be unstable and potentially confusing as to coverage, either by inclusion or non-inclusion.

Moreover, inclusion of particular 'technical information' is unnecessary.

The Act should continue to protect, as personal information about an individual, any information about an individual, technical or otherwise, that is held by a regulated entity in circumstances where the possibility that an individual would be identifiable through an act or practice of that entity in collecting, holding or disclosing that information, and having regard to all other information reasonably available to that entity, is greater than low or remote.

To apply this proposition to *technical information*, if a technical code (cookie, pixel or other online tracking code) on its face is non-identifying but is capable of being associated with information about an individual, the relevant question becomes whether this possibility (that this technical code could be reassociated with personal identifiers through an act or

practice of an entity in collecting, holding or disclosing that information, and having regard to all other information reasonably available to that entity), is greater than low or remote.

If the Act could be revised to more clearly reflect this proposition, that would be a desirable outcome. There would then be less room for confusion as to *personal information about individuals*.

However, consideration of *technical information* needs to be coupled with consideration of *about an individual*. Not all personal information which *relates to* an individual is, or should be, personal information *about* an individual.

Take one example.

An invoice for service of your car may state the name of the mechanic that performed the car service and provide her or his contact details, for the purpose of enabling you (the car owner) to contact the mechanic with any query about the work to the car.

In the context of this invoice about a car, the disclosure of the mechanic's contact details ought not be regarded as a disclosure of personal information about the mechanic, but could fairly be regarded as a disclosure that relates to the mechanic.

If the service centre ought reasonably to anticipate that you (the car owner) will use invoice details to collate and compare the quality of services provided by individual mechanics, the service centre should treat the disclosure as a disclosure of personal information about the mechanic.

If the service centre ought not reasonably anticipate that use, the disclosure should (continue to) be regarded as about a car.

However, if you (the car owner) then took it upon yourself to collate and compare the quality of services provided by individual mechanics, then that activity by you would itself become a collection and use by you of personal information about the mechanics.

In each case, there needs to be consideration of the relevant facts and circumstances of the relevant use or disclosure, and the nature of other information about an individual available to the relevant entity.

Correspondingly, online tracking code may, or may not, be personal information about an individual: it depends upon what other information is reasonably available to the relevant regulated entity (such as availability of a reverse look-up table or other reasonable capability to reassociate that code with personally identifying information about an individual), in all cases evaluated taking into account all relevant controls and safeguards.

The position becomes more complicated when there is a *disclosure*. However, the underlying analysis is, and should remain, contextual.

Consider a scenario where an entity that holds online tracking code, but itself has no capability to reassociate that code with personally identifying information about an individual, discloses that online tracking code and associated attribute data to another entity.

If the relevant circumstances of this disclosure are that the disclosing entity ought to reasonably consider that the recipient entity has the capability to reassociate that code with personally identifying information about an individual (and accordingly the capability to use that attribute data to augment other personal information about a particular individual), this disclosure should be a regulated disclosure of personal information about an individual.

If the relevant circumstances of this disclosure are that the disclosing entity ought to reasonably consider that the recipient entity does not have the capability to reassociate that code with personally identifying information about an individual, this disclosure should be a regulated disclosure of personal information about an individual.

In each case the disclosing entity must put itself in the shoes of each recipient entity that it might reasonably anticipate will have access to the disclosed information. If the disclosure is not subject to technical, operational and legal safeguards and controls that reduce the (objectively assessed) risk of reidentification of relevant individuals (about whom the relevant data set includes data) by each recipient entity, then there is a disclosure of personal information. This is illustrated by the case when the Department of Health released transaction level data capable of reidentification attack by a motivated intruder[4], relevantly Dr Vanessa Teague.[5]

Our submission is that the above summary states the Privacy Act as it stands and operates today. This framework also makes good policy sense. It creates appropriate incentives for organisations:

- to minimise collection, handling and disclosure of personal information about individuals;
- to pseudonymise or otherwise separate personal identifiers from associated information, in order to minimise any risk of inadvertent reidentification, or disclosure through data exfiltration;

[4] If this outcome leads to concern that motivated intruders should not be permitted to attempt to identify individuals within certain publicly released datasets, this Review should consider whether there should be legislated prohibition against such reidentification attempts, as has been legislated in a number of recent national data privacy statutes and was proposed by this Federal Government in its lapsed Privacy Amendment (Re-identification Offence) Bill 2016.

[5] See further Dr Vanessa Teague, Dr Chris Culnane and Dr Ben Rubinstein, University of Melbourne, The Simple Process Of Re-Identifying Patients In Public Health Records, https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records

- to consider technical, operational and legal safeguards and controls that reduce the (objectively assessed) risk of reidentification of relevant individuals (about whom the relevant data set includes data) whenever data sets are made available to another organisation,
- to exercise organisational accountability for data privacy of individuals in relation to data permitted to across multiparty data ecosystems, including by effectively requiring a disclosing entity to 'stand in the shoes' of prospective recipients in evaluating risk of reidentification or other misuse of personal information about individuals through any disclosure which the disclosing entity permits or countenances.

This policy framework also closely aligns with a number of recently revised or pending data privacy statutes, including those of Singapore, South Korea, Canada and Japan.

This policy framework is also consistent with the recently published *Anonymisation Decision-Making Framework: European Legal Context (GDPR) 2nd Edition*.[6] The first edition of this authoritative work formed the basis for the OAIC/Data61 *Deidentification Decision Making Framework*[7] and subsequent (and still current) guidance issued by the Australian Information Commissioner.

3. *Should the definition of personal information be updated to expressly include inferred personal information?*

The current definition addresses information *or an opinion* about an individual.

An inference as to characteristics, interests or preferences of an individual would appear to be an opinion, whether or not statistically valid or justifiable, about an individual.

If there is room for any doubt that an opinion is an inference, then the definition might be clarified.

4. *Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?*

The terms *de-identified*, *anonymised* and *pseudonymised* are not used consistently in Australia.

As a result, there is often misunderstanding as to how the Privacy Act operates in relation to each of them. This undermines good practice in data privacy management by APP entities.

The most common usage is of *deidentified* is as an omnibus term covering both anonymised and pseudonymised information. It would be prudent for Australia to expressly adopt a

[6] https://ukanon.net/framework/
[7] https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework/

similar usage. This usage is becoming increasingly common internationally, although still a long way from universally accepted.

The Glossary to the (pp 107-113) to the *Anonymisation Decision-Making Framework: European Legal Context (GDPR) 2nd Edition*[8] (as to which, see response 1. above) defines relevant terms. Given the utility of common terminology, we set out relevant term descriptions (note: not intended as legal definitions) in that Glossary:

> *De-identification*: The removal or masking of direct identifiers within a dataset.
>
> *Anonymisation*: A complex process to transform identifiable data into nonidentifiable (anonymous) data. This usually requires that identifiers be removed, obscured, aggregated and/or altered in some way. It may also involve restrictions on the data environment.
>
> *Pseudonymisation*: A term defined in GDPR as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is subject to technical and organisational measures to keep it separate.
>
> *Record linkage*: A process by which records about the same population units in different datasets are combined to produce a single dataset
>
> *Re-identification*: The discovery of the concealed identity of one or more individuals in a dataset by using additional relevant information.
>
> *Attribution*: The process of associating a particular piece of data with a particular population unit (person, household business or other entity). Note that attribution can happen with re-identification (if for example all members of a group share a common attribute).
>
> *Disclosure risk*: The probability that an intruder identifies and/or reveals new information about at least one data subject in disseminated data. Because anonymisation is difficult and has to be balanced against data utility, the risk that a disclosure will happen will never be zero. In other words there will be a risk of disclosure present in all useful anonymised data.
>
> *Data release*: Any process of data dissemination where the data controller no longer directly controls who has access to the data. This ranges from general licensing arrangements, such as end user licensing where access is available to certain classes of people for certain purposes, through to fully open data where access is unrestricted.

[8] https://ukanon.net/framework/

> *Data minimisation*: A long-standing data protection principle enshrined in GDPR as a data controller's requirement to ensure that the personal data they hold should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In other words, one should not collect or process more, or more detailed, data than necessary for the purpose.

Two relevant elements of this framework are:

- Because pervasive anonymisation over time is extremely difficult and has to be balanced against data utility, the risk that a reidentification will happen (such as through efforts of a motivated intruder) will never be zero. Anonymisation should not be defined in a way that makes data release impossible. However, the definition should ensure that a regulated entity *is obliged to do all that it reasonably can be expected to do to minimise objectively assessed residual identification risk of deidentified information in the hands of any recipient*.
- *Pseudonymisation* ensures that relevant (deidentified) information is handled in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information where such additional information is subject to technical and organisational measures to keep it separate.

We also note the definition of the "pseudonymlzation" in the proposed *California Privacy Rights and Enforcement Act of 2020*[9] as:

> "the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional Information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer."

(Of course, in the Australian context this definition would need to refer to any individual, not just a consumer.)

In summary, our submission is that *for handling of data to be regarded as a handling of pseudonymised information about an individual:*

1. a regulated entity should be obliged to implement technical, operational and legal safeguards against re-identification of a relevant individual, so that the risk of re-identification of any individual from or in the course of handling of information about that individual by the data analytics services provider is reliably low or remote, and

2. the regulated entity should be obliged not to disclose that pseudonymised information in any form where the risk that any entity (whether the direct recipient or

[9] https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf

another downstream entity) receiving that information could re-identify an individual from that information (using whatever other information that is available to that recipient entity) is greater than reliably low or remote.

To be clear, if a regulated entity discloses (purportedly) deidentified information in any form where the risk that any entity (whether the direct recipient or another downstream entity) receiving that information could re-identify an individual from that information (using whatever other information that is available to that recipient entity) is greater than reliably low or remote, this should be treated as a disclosure of personal information about an individual.

We note in this regard the current guidance of the Australian Information Commissioner:

> The Privacy Act does not require de-identification to remove the risk of re-identification entirely. Rather, those sharing or releasing data must mitigate the risk until it is very low. That is, until there is no reasonable likelihood of re-identification occurring. As part of this, the entity should consider all relevant risks that may impact on the likelihood of re-identification, including the risk of attribute disclosure, and the risk of spontaneous recognition. Entities should also consider the gravity of any harm that could arise from re-identification.[10]

4.3 Flexibility of the APPs in regulating and protecting privacy

6. *Is the framework of the Act effective in providing flexibility to cater for a wide variety of entities, acts and practices, while ensuring sufficient clarity about protections and obligations?*

In a word, *no*.

Like many national data privacy statutes, the Privacy Act is deficient in bridging the gap between ensuring:

- that there is a fair description provided to an affected individual about the purpose and extent of a proposed data collection, use or disclosure or surveillance activity, and
- that this data collection, use or disclosure or surveillance activity is necessary and proportionate to achieve a reasonable outcome, with reasonableness judged by consideration of the degree of risk and extent of impact upon legitimate expectations of privacy, whether an individual suffers a harm that arises from this act or practice, and taking into account societal interests (such as in health and safety of other individuals) and the interests of the regulated entity that wants to collect, use or disclose data in a disclosed and properly risk evaluated way.

[10] https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/

Privacy is commonly described in a general way as t*he interests a person has in controlling what others know about them, in being left alone and in being free from interference or intrusion: the 'right to be let alone'*.[11] This formulation expands upon the Warren and Brandeis (1890) summation of privacy as the 'right to be let alone'[12] and focusses upon the *seclusion* and *separation* elements of privacy.

It is not necessary to see privacy as a *right* in order to recognise the *legitimate interests (reasonable expectations and claims)* of affected persons to be legally entitled to determine (not own) when, how, and to what extent information about them is communicated.

As the Privacy Act stands, the concepts of:

- responsibility and accountability of APP entities in their management of personal information about individuals,
- reasonableness and fairness of an act or practice of an APP entity in their management of personal information about individuals, with reasonableness and fairness determined having regard to:
    - ♦ rights or legitimate interests of affected individuals in protection of their data privacy,
    - ♦ societal interests in protection of the privacy of individuals, and
    - ♦ interests of entities in carrying out their functions or activities,

are not expressly relevant considerations in determining whether and when there is an *interference with the privacy of an individual.*

Our submission is that this Review should address these deficiencies.

For clarity, we note that *risk* is used in the Act in two ways that are not relevant to this submission: first, in the sense of insurance risks and credit risks, and second, in the concept of individuals who are *at risk* from an eligible data breach. However, *risk* is not used in the Act in two senses relevant to this submission, being:

- an assessment measure (level of possibility of harm occurring), and
- as a differentiator of privacy risks from other types of risks.

Harm is used in the Act only in (or in relation to) *Part IIIC Notification of eligible data breaches* of the Act, in the context of a breach being an eligible data breach where,

[11] See further Cohen, Julie, 'What is Privacy For', (2013) 126 Harvard Law Review 1904; Nissenbaum, Helen, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford, CA, Stanford Law Books, 2010; Colin J Bennett, 'In Defence of Privacy: The concept and the regime', (2011) 8 Surveillance and Society 485

[12] Warren, Samuel and Louis Brandeis, "The Right to Privacy", (1890) Harvard Law Review 193

relevantly, "a *reasonable person* would conclude that the access or disclosure would be *likely to result* in *serious harm to any of the individuals to whom the information relates*".[13] In the context of determining whether a data breach is notifiable, the Act informs an APP entity as to relevant matters to have regard to in determining whether access or disclosure would be likely, or would not be likely, to *result in serious harm*.[14]

The Explanatory Memorandum informs us that "the 'reasonable person' and 'likely risk' elements of the notification standard, by using commonly-understood legal standards of objectivity and probability, are intended to provide greater certainty for regulated entities while maintaining consistency with the core element of the ALRC recommendation" (of a 'real risk of serious harm' standard)[15].

The Explanatory Memorandum also informs us that:

> Serious harm, in this context, could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach. Though individuals may be distressed or otherwise upset at an unauthorised access to or unauthorised disclosure or loss of their personal information, this would not itself be sufficient to require notification unless a reasonable person in the entity's position would consider that the likely consequences for those individuals would constitute a form of serious harm.[16]

However, we are not provided with any definitions or other statutory guidance as to which possible *harms* to individuals are relevant or how to assess the threshold at which a harm becomes a *serious harm.*

Instead, the Privacy Act 1988 generally links "privacy" to requirements imposed upon APP entities through an intermediate concept of *interference with the privacy of an individual.*

Section 13 states:

> 13 Interferences with privacy
>
> (1) An act or practice of an APP entity is an *interference with the privacy of an individual* if:
>
> (a) the act or practice breaches an Australian Privacy Principle in relation to personal information about the individual; or

[13] Section 26WF(2)
[14] Section 26WG
[15] Explanatory Memorandum to the Privacy Amendment (Notifiable Data Breaches) Bill 2016, paragraph [8]
[16] Explanatory Memorandum to the Privacy Amendment (Notifiable Data Breaches) Bill 2016, paragraph [9]

(b) the act or practice breaches a registered APP code that binds the entity in relation to personal information about the individual.

Other provisions deem a particular act or practice as specified in those respective provisions to be an *interference with the privacy of an individual* and thereby link impermissibility of a particular act or practice to penalty and enforcement provisions.

This creates a fundamental structural flaw in a statute that must now be applied in a data and AI enabled economy. Many activities of organisations, including but not only provision of products and services:

- generate, sometimes merely as an incidental by-product (digital exhaust), or
- consume (use as a relevant input), or
- transform and create outputs from, or
- any combination of the above,

personal information about individuals.

As the regulatory framework is built upon requirements that APP entities:

- provide notice and choice, or notice and consent, and
- manage personal information in an open and transparent way,

APP entities must consider and evaluate rights and interests of individuals in and to privacy, and possible harms to individuals, without any statutory guide or assistance as to:

- identification of privacy risks or privacy harms or
- measurement and management of level or impact or harms.

The requirements as to transparency and notice apply without any threshold criteria as to:

- what individuals might reasonably be expected to know or indeed require as an inherent attribute of a particular activity of an APP entity (being an activity that the affected individual wants the APP entity to do),
- reasonable expectations of affected individuals,
- “reasonableness” or “fairness” as often used elsewhere in the law as an objective standard.

Although Australian privacy regulators and privacy professionals often talk about ‘privacy risk management’ and ‘privacy impact assessment’, the Act does not describe what is a *privacy risk*, what is a *privacy impact*, what is *an appropriate process for risk or impact assessment, mitigation or management*, or (to take a more specific example) what is *the*

relevance or otherwise of controls and safeguards implemented by an APP entity in relation to the handling of personal information.

Meanwhile, conferences and other forums of global data protection and privacy regulators and experts devote an increasing proportion of their time discussing:

- newly emerging best practice as to privacy risk management frameworks,
- privacy risk assessment,
- special assessment for 'higher risk processing', and
- responsibility and accountability of regulated entities for data risks created by or within multi-party data ecosystems that particular regulated entities manage or provide.

A similar, but more graduated approach is promoted by the Information Accountability Foundation (**IAF**) in the IAF's Model Legislation.[17] This draft Act is built upon two foundational principles, elaborated in a two page introductory section (Section 102, Findings and Purpose)[18] and in outline:

- the benefits of the information age belong to everyone; and
- in today's data-driven economy, organizations must be responsible stewards of personal data and be accountable for their actions.

Although the term "harm" is not expressly used in the Model Legislation, it uses an analogous concept of "adverse processing impacts", and provides a non-exhaustive list of examples of "adverse processing impacts" (being a list derived from the oft-cited 'taxonomy of privacy harms' attributed to Professor Daniel Solove[19]. Relevant key concepts are described in the IAF's Model Legislation as follows:

> *"adverse processing impact*, meaning the detrimental, deleterious, or disadvantageous consequences to an individual arising from the processing of that individual's personal data or to society from the processing of personal data.
>
> *processing risk*, meaning the level of adverse processing impact potentially created as a result of or caused by processing, a specific processing activity, or a specific processing action, assessed as a function of the customary factors, being:

[17] Variously referred to by the Information Accountability Foundation as the *Fair Accountable Innovative Responsible and Open Processing Enabling New Uses that are Secure and Ethical Act*, the *FAIR and OPEN USE Act* or the *Model Legislation*, and available through https://informationaccountability.org/publications/ at https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/FairOpenUseAct.9.23.19.FINAL-V2-1.pdf

[18] Sept. 23, 2019 draft, at lines 81-170

[19] Solove, Daniel J., "A Taxonomy of Privacy", 154 U. Pa. L. Rev. 477, 526–29 (2005)

(A) the likelihood that adverse processing impact will occur as a result of processing, a specific processing activity, or a specific processing action; and

(B) the degree, magnitude, or potential severity of the adverse processing impact, should it occur."

The definition of *adverse processing impact* includes a non-exhaustive list of examples as follows:

"(1) direct or indirect financial loss or economic harm,

(2) physical harm,

(3) psychological harm, including anxiety, embarrassment, fear, and other mental trauma,

(4) inconvenience or expenditure of time,

(5) a negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit related to employment (including hiring, firing, promotion, demotion, reassignment, or compensation), credit and insurance (including denial of an application, obtaining less favourable terms, cancellation, or an unfavourable change in terms of coverage), housing, education, professional certification, issuance of a license, or the provision of health care and related services,

(6) stigmatization or reputational harm,

(7) disruption and intrusion from unwanted commercial communications or contacts,

(8) price discrimination,

(9) effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relate, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity assessing adverse processing impact, that materially—

(A) alter that individual's experiences,

(B) limit that individual's choices,

(C) influence that individual's responses, or

(D) predetermine results or outcomes for that individual,

(10) other detrimental or negative consequences that affect an individual's private life, including private family matters, actions, and communications within an individual's

home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected, observed, or used; and

(11) with respect to detrimental, deleterious, or disadvantageous consequences to society arising from processing personal data, such other demonstrable consequences that may negatively impact a community or the public, taking into account factors such as national security, consumer confidence, the effective and efficient operation of government, effect on the public welfare, or ongoing or disproportionate allocation of risk on a particular population or community."[20]

When assessing the potential severity and likelihood of adverse processing impact, the Model Legislation requires a covered entity to consider context, including the purpose for the processing, sensitivity of the personal data, 'linkability' and 'identifiability' of data, the sources of information.

4.4 Exemptions

Small business exemption

7. *Does the small business exemption in its current form strike the right balance between protecting the privacy rights of individuals and avoid imposing unnecessary compliance costs on small business?*

No, the current small business exemption does not strike an appropriate balance between reducing business compliance costs and protecting data privacy of individuals.

Processes and practices for compliance with the Privacy Act are now quite well understood and therefore should no longer be a significant compliance cost for businesses that collect and handle personal information as an incident of their core business.

Where handling of personal information is a core business activity, the carve-in from the small business exemption generally means that the Privacy Act already operates.

In any event, most cases small businesses do not pay or otherwise give an individual any material benefit for collection or use of their personal information. Without any data privacy obligations being imposed on small businesses, individuals are at a significant disadvantage and are subject to personal information about them being exposed without protection. The benefit that businesses gain from collection and handling of personal information generally should mean that that the burden of compliance with the Privacy Act is a reasonable cost of doing business fairly and responsibly.

Of course, any change requires sensible change management, including provision of guidance, training and other assistance.

[20] Sept. 23, 2019 draft, at lines 173-211

The Commissioner should also be authorised to make class exemptions from particular requirements of the Privacy Act if in practice compliance with specific obligations proves unduly burdensome for small businesses as a class.

Employee records exemption

13. *Is the personal information of employees adequately protected by the current scope of the employee records exemption?*

No.

In any event, the exemption is not well understood and many employers assume that it applies in circumstances where it does not.

However, the concept of (voluntary) consent in relation to employees is problematic.

We submit that the employee records exemption should be removed, but in conjunction with introduction of an appropriately framed and over-arching:

- legitimate interests exception, which should include within its scope reasonable record keeping by APP entities as a reasonable incident of engagement, management (both personnel management and reduction of business risk) and disengagement of staff (both employees and independent contractors) by APP entities, and
- "appropriate purpose" requirement – see further section 2 above of this submission.

Political parties exemption

16. *Should political acts and practices continue to be exempted from the operation of some or all of the APPs?*

Political parties and those engaging in political acts and practices should be subject to the Privacy Act, provided that the provisions accommodate the constitutional doctrines of implied freedom of political communication and parliamentary privilege.

When the Australian Law Reform Commission (**ALRC**) conducted its review of the Privacy Act in 2008, the ALRC recommended that the political exemptions should be abolished.[21] As with many of the recommendations in the report, this recommendation was not implemented.

As Professors Moira Paterson and Normann Witzleb have demonstrated[22], over the period since that 2008 recommendation, uses of data analytics by political parties for data mining

[21] Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' (2008) ALRC Report 108, Rec 41-1

[22] Moira Paterson and Normann Witzleb, Chapter 1, Political micro-targeting in an era of big data analytics: An overview of the regulatory issue, and Chapter 9: Voter privacy in an era of big data, Time to abolish the political exemption in the Australian Privacy Act; in Janice Richardson, Normann Witzleb and Moira Paterson,

of social media and microtargeting of voters have increased the need for transparency of handling of personal information by political parties.

A recent audit by the UK Information Commissioner's Office (**UK ICO**) of how UK political parties are handling voter information surfaced lack of compliance across the political spectrum with UK data protection rules:

> "Political parties have always wanted to use data to understand voters' interests and priorities, and respond by explaining the right policies to the right people. Technology now makes that possible on a much more granular level. This can be positive: engaging people on topics that interest them contributes to greater turnout at elections. But engagement must be lawful, especially where there are risks of significant privacy intrusion – for instance around invisible profiling activities, use of sensitive categories of data and unwanted and intrusive marketing. The risk to democracy if elections are driven by unfair or opaque digital targeting is too great for us to shift our focus from this area."[23]

We also note the September 2018 "Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners Securing Trust and Privacy in Canada's Electoral Process"[24], as follows:

> "Recent high-profile investigations in the United Kingdom, the United States, New Zealand and elsewhere reveal that political parties are gathering significant amounts of personal information on voters as they adopt micro-targeting techniques.
>
> Political parties also hold personal information on volunteers, employees and candidates.

(Eds.), Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-targeting (1st ed), Routledge, https://doi.org/10.4324/9780429288654-1

[23] Information Commissioner's Office (UK), Audits of data protection compliance by UK political parties, Summary report, November 2020, available at https://ico.org.uk/media/action-weve-taken/2618567/audits-of-data-protection-compliance-by-uk-political-parties-summary-report.pdf; Media Release 11 November 2020, UK political parties must improve data protection practices, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/uk-political-parties-must-improve-data-protection-practices/; see also Investigation into the use of data analytics in political campaigns: A report to Parliament, 6 November 2018, https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf. See also Sabrina Wilkinson, Voter Privacy: What Canada can learn from abroad, Open Canada, 4 October 2019, https://opencanada.org/voter-privacy-what-canada-can-learn-abroad/; Office of the Privacy Commissioner of Canada, Investigation finds BC firm delivered micro-targeted political ads without ensuring consent, 26 November 2019, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/nr-c_191126/; Elections Canada, Applying Fair Information Principles to Political Parties – Discussion Paper 3: The Protection of Electors' Personal Information in the Federal Electoral Context https://www.elections.ca/content.aspx?section=res&dir=cons/dis/compol/dis3&document=p5&lang=e, http://dx.doi.org/10.2139/ssrn.3589687l

[24] Available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_180913/

These practices have the potential to significantly impact the privacy of citizens and undermine their trust in the democratic system.

At present, British Columbia is the only jurisdiction in Canada where political parties are subject to privacy legislation. It is also the only province where voters can complain to an independent body about a political party's privacy practices.

The federal government tabled Bill C-76 (the Elections Modernization Act) earlier this year requiring registered federal political parties to develop privacy policies and publish them online.

However, Bill C-76 does not establish standards for political parties to follow in the handling of personal information nor does it establish an independent body which would oversee how their privacy practices are implemented.

WHEREAS

Privacy is a fundamental human right that enables the freedom of association, thought and expression, including political affiliation, participation and debate.

Canadian courts have consistently affirmed the importance of these fundamental rights.

Much of the personal information gathered by political parties on electors, such as political views and voting intentions, is sensitive.

Personal information on electors, employees, volunteers or candidates gathered by political parties should be subject to privacy protections..

Political parties outside of British Columbia are not required by law to protect the personal information they collect, nor is their handling of Canadians' personal information subject to review by an independent body.

Privacy Commissioners, Chief Electoral Officers, legislators, academic experts, non-governmental organizations and newspaper editorial boards have recommended oversight of the privacy practices of political parties.Footnote4

Canadians have overwhelmingly stated they wish to see political parties made subject to privacy laws.

THEREFORE

The Federal, Provincial and Territorial Privacy Commissioners of Canada urge their respective governments to ensure Canadian law at all levels carries meaningful privacy obligations for political parties by passing legislation:

Requiring political parties to comply with globally recognized privacy principles;

Empowering an independent body to verify and enforce privacy compliance by political parties through, among other means, investigation of individual complaints; and,

Ensuring that Canadians have a right to access their personal information in the custody or control of political parties."

Journalism exemption

17. *Does the journalism exemption appropriately balance freedom of the media to report on matters of public interest with individuals' interests in protecting their privacy?*

No.

The journalism exemption, as introduced in 2000 (when the Privacy Act was extended to businesses), was designed to cover 'traditional media outlets' at the time.[25]

Section 7B(4) of the Act provides that an act or practice of a "media organisation" is exempt if done "in the course of journalism" and provided the media organisation is "publicly committed" to "observe standards" that "have been published in writing by the organisation or a person or body representing a class of media organisations".

This is a curious case of media organisations being able to write their own exemption, without any precondition of review or approval by any third party, regulator or otherwise. The exemption was inappropriate when enacted. Today it is simply archaic.

It should be an obvious statement of fact that a data privacy right without remedy other than a remedy (if any) as a media organisation may elect to offer if that media organisation's preferred statement of standards provides a remedy to an affected individual and the organisation elects to comply with that requirement, is not a right of legal substance.

Assertion of legitimate expectations of individuals to personal privacy should not be allowed to chill fair but vigorous reporting and open democracy. However, it is inappropriate that review and oversight of a media organisation's balancing of public interest, and of legitimate expectations of privacy of individuals, to be left solely in the hands of media organisations.

Media organisations conducting journalism are inherently conflicted in any evaluation of interest of the public in a story and a legitimate expectation of an individual in their personal privacy. This statement is not a criticism of Australian mainstream media or its reporting. It is a statement of obvious fact that getting a story about activities of individuals

[25] See further Sally McCausland, Journalism, The Arts and Data Protection: The Potential Reach of the Privacy Act, Communications Law Bulletin Vol 36.2 (June 2017)

that individuals do not wish to be reported often entails a journalist navigating a narrow path between illegitimate claims, and legitimate expectations, of privacy of individuals. I

The exemption covers (only) a “media organisation” whose activities include the collection or dissemination of “material having the character of news, current affairs, information or a documentary” or of commentary or opinion on such material.

"Media organisation" includes the word “organisation”, leaving a question as to whether the exemption applies to citizen journalists or operating their own businesses publishing material that otherwise has the necessary character of journalism. This appears anomalous and inequitable.

The concepts of media and journalism should be combined and cover reportage which has the character of news, current affairs, information or a documentary, or commentary or opinion on, or analysis of, news, current affairs, information or a documentary, for the purpose of making it available to the public.

Comparable jurisdictions exhibit different approaches to a journalism exception from operation of a data privacy statute.

The UK Data Protection Act 1998 provides “Exemptions etc based on Article 85(2) [of the GDPR, addressing “processing carried out for journalistic purposes”[26]] for reasons of freedom of expression and information” for the processing of personal data if the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material, and the data controller reasonably believes that the publication of the material would be in the public interest.[27]

In a February 2019 judgment[28] of the Court of Justice of the European Union (**CJEU**), the CJEU found that citizen journalists, such as bloggers, also can rely on the derogation [*derogation* being GDPR jargon for *exemption*] for journalistic purposes.

In determining whether publication would be in the public interest, the controller must take into account the special importance of the public interest in the freedom of expression and information. In determining whether it is reasonable to believe that publication would be in

[26] For a detailed recent review of the operation of this derogation, see Natalija Bitiukova, Journalistic Exemption Under The European Data Protection Law, Policy Paper of the Vilnius Institute for Policy Analysis, 2020

[27] Schedule 2, Part 5, section 26: https://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/5/enacted

[28] *Sergejs Buivids v. Datu valsts inspekcija*, ECLI:EU:C:2019:122, http://curia.europa.eu/juris/document/document.jsf?docid=210766&doclang=EN. The judgement related to Article 9 of Directive 95/46, but that Article is very similar to Article 85 GDPR. Contrast France: pursuant to Article 80 of the French data protection act, only professional journalists can rely on the derogation for journalistic purposes. This French provision may no longer be considered compliant with GDPR.

the public interest, the controller must have regard to any of the codes of practice or guidelines listed in section 26(6) that is relevant to the publication in question, being:

- BBC Editorial Guidelines;
- Ofcom Broadcasting Code;
- Editors' Code of Practice.

The Data Protection Act 2018 also requires the Commissioner to produce a code of practice that "provides practical guidance and promotes good practice in regard to processing personal data for the purposes of journalism". This (data protection and journalism) code is one of four statutory codes that the UK ICO is required to publish under the Data Protection Act 2018, the others being the age appropriate design code (published in August 2020), the data-sharing code (draft in consultation) and the direct marketing code (draft in consultation). The UK Information Commissioner conducted a public consultation as to a draft Code, which consultation closed in May 2020.[29] The writer's understanding is that the final Code has not been published (as at 18 December 2020).

New Zealand recently renewed an exemption for "a news entity", to the extent that it is "carrying on news activities": section 8(b)(x) of the New Zealand Privacy Act 2020.

"News activity" is defined as gathering, preparing, or compiling, for the purposes of publication, any news, observations on news and current affairs, and publishing any news, observations on news and current affairs.

The writer reads this definition as intended to include databases gathered in the course of investigative journalism or for obituaries or as backgrounders for journalists, and hence intended to exclude rights of access and correction of affected individuals. This review should consider a definition of news activity appropriate to cover activities preparatory for and reasonably incidental to publication of news as broadly defined.

"News entity" is defined as an entity (including an individual) whose business, in whole or part, consists of a news activity; and that is, or is employed by an employer that is, subject to the oversight of the Broadcasting Standards Authority; or the New Zealand Media Council; or an overseas regulator providing an independent procedure for the consideration and adjudication of privacy complaints that is accessible to complainants, including complainants residing in New Zealand; or any other body prescribed as a regulatory body by regulation.

[29] https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-on-a-data-protection-and-journalism-code-of-practice/; see consultation summary at https://ico.org.uk/media/about-the-ico/consultations/2029/consultation-response-summary-dp-and-journalism-a-guide-for-the-media.pdf

An analogous approach would be to exempt Australian news entities, to the extent carrying on news activities, to the extent subject to the oversight of the Australian Communications and Media Authority or similar overseas regulator (and subject to the same proviso).

An alternative approach would be to exempt an entity (which might include an individual), in relation to news activities (but not its other activities), to the extent that the entity publicly and prominently commits to comply with, and does comply with:

- a code of practice reviewed, approved and registered by the OAIC, or the Australian Communications and Media Authority; or
- a standard determined by the OAIC, or the Australian Communications and Media Authority.

As a precondition to operation of a code of practice or standard, a code or standard should provide for appropriate independent oversight, confer appropriate remedies that may be sought by affected individuals, and include rights of appeal to a fully independent review body.

As to the processes for consultation and review as a precondition for registration of a relevant code, we commend sections 32 to 38 of the (New Zealand) Privacy Act 2020 for consideration in this Review.

18. *Should the scope of organisations covered by the journalism exemption be altered?*

Yes.

The exemption should apply to an entity (which might be an individual), in relation to news activities (but not its other activities), to the extent that it publicly and prominently commits to comply with an approved and registered code or standard, as described in the above response to Q17.

19. *Should any acts and practices of media organisations be covered by the operation of some or all of the APPs?*

All activities of media organisations should be covered by the APPs, subject only to the exemption.

4.5 Notice of Collection of Personal Information

Improving awareness of relevant matters

20. *Does notice help people to understand and manage their personal information?*

The Joint Committee on Human Rights of the UK House of Commons and House of Lords, in its Report on The Right to Privacy (Article 8) and the Digital Revolution[30], concluded:

> "The evidence we heard during this inquiry, however, has convinced us that the consent model is broken. The information providing the details of what we are consenting to is too complicated for the vast majority of people to understand. Far too often, the use of a service or website is conditional on consent being given: the choice is between full consent or not being able to use the website or service. This raises questions over how meaningful this consent can ever really be.
>
> Whilst most of us are probably unaware of who we have consented to share our information with and what we have agreed that they can do with it, this is undoubtedly doubly true for children. The law allows children aged 13 and over to give their own consent. If adults struggle to understand complex consent agreements, how do we expect our children to give informed consent? Parents have no say over or knowledge of the data their children are sharing with whom. There is no effective mechanism for a company to determine the age of a person providing consent. In reality a child of any age can click a 'consent' button.
>
> The bogus reliance on 'consent' is in clear conflict with our right to privacy. The consent model relies on us, as individuals, to understand, take decisions, and be responsible for how our data is used. But we heard that it is difficult, if not nearly impossible, for people to find out whom their data has been shared with, to stop it being shared or to delete inaccurate information about themselves. Even when consent is given, all too often the limit of that consent is not respected. We believe companies must make it much easier for us to understand how our data is used and shared. They must make it easier for us to 'opt out' of some or all of our data being used. More fundamentally, however, the onus should not be on us to ensure our data is used appropriately - the system should be designed so that we are protected without requiring us to understand and to police whether our freedoms are being protected.
>
> As one witness to our inquiry said, when we enter a building we expect it to be safe. We are not expected to examine and understand all the paperwork and then tick a box that lets the companies involved 'off the hook'. It is the job of the law, the regulatory system and of regulators to ensure that the appropriate standards have been met to keep us from harm and ensure our safe passage. We do not believe the internet should be any different. The Government must ensure that there is robust regulation over how our data can be collected and used, and that regulation must be stringently enforced."

[30] HC 122, HL Paper 14, published on 3 November 2019

Most data privacy laws are intended to empower individuals by informing them how data about them may be being collected and used, and thereby enable them to exercise a choice. This foundation of 20th century data privacy regulation is variously called the 'notice and consent', 'notice and choice', 'individual choice' or 'privacy self-management' framework. The mechanism to give effect to this foundational theory is a requirement that each regulated entity:

- make available a privacy policy that explains generally how it deals with personal data,
- provides to an affected individual a more specific and targeted privacy notice at or near the point or time of collection of particular personal data, and
- seeks consent in relation to collection and uses of certain specified categories of more sensitive personal data. This is the "notice and choice", or "notice and consent", framework for data privacy regulation.

Most national data privacy statutes remain firmly rooted in the notice and choice framework. Indeed, many recent data privacy statutes double-down on the level of information that must be provided to individuals, with the stated objective of facilitating individual choice, notwithstanding the body of evidence accumulating since about the year 2000 that the notice and choice framework is failing.

Critiques of this foundational theory for data privacy regulation focus upon the 'illusion of consent', as described by Paul Ohm and other privacy scholars, or the more recent restatement (by Dan Solove and others) of this illusion as 'the privacy self-management problem'. In brief, these criticisms revolve around the problem of expecting affected individuals to properly understand and make a choice about whether to accept an act or practice which affects the individual's privacy, and particularly when there is often no practical ability for each of us to say *no*, or even *no to that, but it might be OK if you did it this way other way…[insert here*].

Critiques of "notice and choice" generally suggest that this framework needs to be supplemented, or replaced, by an additional requirement of demonstrated organisational accountability of the entity that is collecting, handling or disclosing personal information about the affected individual, or instituting surveillance of a human, identifiable or not. As has been advocated in sections 2 and 3 above of this submission.

21. *What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?*

We suggest a new APP 5.3 along the following lines:

(a) An APP 5 notice must be concise, transparent, intelligible and easily accessible, written in clear and plain language, provided free of charge, and must clearly set out how the APP entity will collect, use and disclose personal information about

an affected individual. Where the personal information of children is intended or otherwise likely to be collected, the notice should be written at a level that can be readily understood by the minimum age of the reasonably likely audience of affected individuals.

(b) A notice must be in a format that draws the affected individual's attention to the notice and is readable, including on smaller screens, if applicable.

(c) A notice must be reasonably accessible to consumers with disabilities.

(d) A notice may be layered or link to other documents, provided that these other layers and other documents are intelligible and easily accessible.

(e) If an entity collects personal information about an individual that an individual would not reasonably expect to be collected, the entity must provide a prominent just-in-time notice including a summary of the categories of personal information being collected and a link to the full notice at collection. [31]

4.6 Limiting information burden

24. *What measures could be used to ensure individuals receive adequate notice without being subject to information overload?*

There should be carefully crafted exceptions for legitimate interests, including reasonable business purposes.[32]

The Commissioner should have broader powers to adjust requirements of the Act to reduce regulatory burdens in particular circumstances where those burdens are not required to achieve the objects of the Act.

The guidance related functions of the Australian Information Commissioner under s 28(1) of the Privacy Act should be expanded to include the power to make guidelines or directions as to application of one or more of the APPs in and to a specified class of circumstances as specified in that guideline or direction, which guidelines or directions have the effect of modifying, including but not only by way of restriction or limitation or imposition of

[31] The draft CCPA Regulations provide as an example "if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, which contains the information required by this subsection".

[32] See for example Part 3 of the new First Schedule to the Personal Data Protection Act of 2012 (**PDPA**) of Singapore, as amended in November 2020 by the Personal Data Protection (Amendment) Act 2020 (gazetted 10 December 2020 and pending commencement), and the *Draft Advisory Guidelines On Key Provisions Of The Personal Data Protection (Amendment) Bill* issued 20 November 2020 by the Personal Data Protection Commission (PDPC) of Singapore: https://www.pdpc.gov.sg/guidelines-and-consultation/2020/11/draft-advisory-guidelines-on-key-provisions-of-the-personal-data-protection-(amendment)-bill.

additional requirements, the application or operation of one or more of the APPs, including but not only the application or operation of APPs 1 and 5.

Examples of permitted modifications might include specification of circumstances:

(a) as when and how information stated in an APP privacy policy pursuant to APP 1 is not required to be again stated in a privacy notice provided to an affected individual pursuant to APP 5.1 as to matters in APP 5.2,

(b) as whether, when and how an APP entity must give notice to an affected individual as to collection or other handling of personal information about that individual,

(c) as to the form and other characteristics of any notice, including the use of links or cross-references to other text, multi-layered notices, standard definitions, phrases, language or icons,

(d) as whether, when and how an APP entity must obtain consent of an affected individual to a particular collection or other handling of personal information about an individual,

(e) as to the form and content of disclosures to be made by an APP entity to an individual before the consent of that individual is provided,

(f) as to the circumstances in which a consent is valid, or in which a consent will not be valid,

(g) as to the form and other characteristics of any consent, including use or graduated consent or tiered consent

(h) as to the manner of seeking, obtaining and evidencing consent.

4.7 Consent to collection and use and disclosure of personal information

26. *Is consent an effective way for people to manage their personal information?*

No.

Consent fatigue is a significant problem.

If a regulated entity is required to seek and obtain consent, for the currently foreseeable future consumer behaviour is such that the regulated entity can expect that many or most affected individuals are likely to give consent, regardless of the range of circumstances for which consent is obtained.

The regulated entity is therefore incentivised to seek consent for and in relation to an expanded range of uses and disclosures.

It follows that effecting 'consumer choice' and 'consumer control' through expansion in requirements for regulated entities to seek and obtain consent may be a sub-optimal regulatory option, as compared to regulatory settings and controls which provide incentives for a regulated entity to minimise collection, use and sharing of personal information about individuals.

Further, imposing further burdens upon affected individuals to determine whether to give or refuse consent is more likely to entrench established advantage of certain online services, and in particular vertically or horizontally integrated 'one stop shops' such as certain smartphone data providers, global social media platforms, search engines, cloud consumer services, online commerce sites. This is partly because many users perceive[33] that they are dependent upon such services and are therefore more likely to give consent to such providers than providers of services that the user perceives as less essential, such as disaggregated (niche or specialised) or local services.

A further perverse outcome of regulatory action expanding consent requirements - perverse because it is detrimental to consumer welfare - may be to stimulate development of consent enabled walled gardens that further entrench and advantage services of certain large providers.

By contrast, imposition of accountability requirements upon data collectors and data users is likely to effect more fairly distributed supply-side outcomes, as accountability assessment and measures can be effected by smaller regulated entities at manageable cost. This cost is also likely to decline as impact assessment and information accountability frameworks, methodologies and processes became standardised and mature, more widely understood, and the pool of experienced advisers able to assist entities to implement organisational accountability grows.

Requirements for consent should be focussed upon circumstances where consent is really needed, being:

- collections, uses and disclosures of personal information about affected individuals that create a real risk of causing significant harm, having regard to remaining or residual risks having after a regulated entity has taken appropriate mitigation measures, and

[33] "The decision is typically all-or-nothing: accept the terms and conditions set forth in the terms of service (TOS) or end-user license agreement (EULA) or do not engage with the product or service at all. And the latter is often not a realistic option, because the perceived cost of opting out is often too high. If, for instance, the choice is between accepting a social network's privacy policy and getting to see pictures of one's grandchildren, or rejecting the policy's terms and not getting to see them, many grandparents will not view the latter as an acceptable option. As Helen Nissenbaum puts it: "While it may seem that individuals freely choose to pay the informational price, the price of not engaging socially, commercially, and financially may in fact be exacting enough to call into question how freely these choices are made": Susser, Daniel, "Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't", Journal of Information Policy, Vol. 9 (2019), pp37-62

- collections, uses and disclosures that are reasonably likely to be unexpected.[34]

The recent amendments to the PDPA of Singapore introduce two new forms of deemed consent:

a) Deemed consent by contractual necessity. This is where consent is deemed for the disclosure of personal data from one organisation to another for the necessary conclusion or performance of a contract/transaction between the individual and the organisation he had originally provided the personal data to; and

b) Deemed consent by notification. This is where consent is deemed from an individual's acquiescence after notification and where the notification is in compliance with certain requirements.

The concept of deemed consent by notification is risk based. In order to rely on deemed consent by notification, organisations are required to assess and ascertain that the intended collection, use or disclosure of personal data for the purpose is not likely to have any adverse effect on the individual after implementing measures to eliminate, reduce the likelihood of or mitigate the identified adverse effect to the individual.

Organisations also may not rely on this approach to obtain consent to send direct marketing messages to the individuals.

Individuals will also be able to withdraw their consent to the collection, use or disclosure of their personal data.[35]

30. *What requirements should be considered to manage 'consent fatigue' of individuals?*

We recommend that the Privacy Act (including APP 6) be amended along the following lines:

[34] Compare section 3.02 (Meaningful Control) of the 23 September 2019 draft of the IAF Fair and Open Use Act "(b) HIGH RISK PROCESSING.—A covered entity should, where practicable, obtain informed consent from an individual before a covered entity processes that individual's personal data if the processing is reasonably likely to create a high level of processing risk. (c) EXTREME RISK.—Unless otherwise provided by law, a covered entity shall obtain informed consent from an individual before a covered entity processes that individual's personal data where the processing is reasonably likely to create an extreme level of processing risk"; and American Law Institute, (draft) Principles of Law, Data Protection, Articles §4(e)(1) and (g)(2) ("for any data activity that is significantly unexpected or that poses a significant risk of causing material harm to a data subject…. only clear and affirmative consent shall suffice for valid consent. Clear and affirmative consent cannot be inferred from inaction".")

[35] See further paragraphs [2.14] to [2.19] of the *Draft Advisory Guidelines On Key Provisions Of The Personal Data Protection (Amendment) Bill* issued 20 November 2020 by the Personal Data Protection Commission (PDPC) of Singapore: https://www.pdpc.gov.sg/guidelines-and-consultation/2020/11/draft-advisory-guidelines-on-key-provisions-of-the-personal-data-protection-(amendment)-bill

Consent of an affected individual is not required to the extent that that purpose of collection, use or disclosure of personal information about an individual and any directly related secondary purpose, is:

(a) for a permitted general situation or a permitted health situation, to the extent that the relevant collection, use of disclosure of personal information is necessary and proportionate in relation to that permitted general situation or a permitted health situation; or

(b) for an other permitted situation where:

(i) the collection, use of disclosure of personal information is necessary and proportionate in relation to that other permitted situation, and

(ii) the regulated entity has established, implemented, tested, revised, and documented reasonable and appropriate policies, procedures and technical, operational and legal controls and safeguards, taking into account this purpose of the processing and the level of processing risk; and

(iii) that other permitted situation is one of the following:

(A) a **fair ongoing entity process**, being a collection, use, or disclosure to facilitate, improve, or safeguard the logistical or technical ability of the APP entity to provide goods or services to the affected individual, to manage operations of the APP entity or to protect against risk, including the collection, use or disclosure of personal information only to the extent reasonably required:

- to provide, operate, or improve a specific product or service required used, requested, or authorized by the individual, including the ongoing provision of customer service and support;
- to analyse the individual's use of a product or service provided by the covered entity to improve the APP entity's products, services, or operations;
- support basic business functions that enable an APP entity to operate efficiently, such as accounting, billing, payment processing, inventory and supply chain management, warranty fulfillment, human resource management, quality assurance, and internal auditing;

- for any other purpose specified in a direction given by the Information Commissioner for the purpose of this provision;

or

(B) any other permitted situation as may be specified as such in the regulations / a direction given by the Information Commissioner for the purpose of this provision.

4.8 Exceptions to the requirement to obtain consent

31. *Are the current general permitted situations and general health situations appropriate and fit-for-purpose? Should any additional situations be included?*

We suggest that the existing categories of permitted general situations and permitted health situations are brought within a category of 'legitimate uses', which:

- do not require notice or consent,
- must comply with the proposed additional requirement as to "appropriate purpose" (see section 2 above),
- should include a broader personal and public health and safety sub-category (i.e. the use is necessary to protect the health or safety of the individual, a group of individuals, or larger community, taking into account the totality of the circumstances pertaining to a particular threat, including cooperation with law enforcement agencies concerning conduct or activity that the APP entity reasonably believes may contravene a law of the Commonwealth, a State or a Territory),[36]
- should include a broader information security sub-category (i.e. the use is necessary to protect the security of devices, networks, or facilities against malicious, fraudulent or illegal activity, or to prosecute those responsible for that activity),[37] and
- should include an ongoing business processes exception.[38]

4.9 Pro-consumer defaults

32. *Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?*

[36] Compare the definition of 'Public Health and Safety' at page 15, lines 418-423 of the 23 September 2019 draft of the IAF Fair and Open Use Act

[37] This drafting reflects the definition of 'Information Security' at page 14, lines 398-400 of the 23 September 2019 draft of the IAF Fair and Open Use Act

[38] See, for example, the "business improvement" use exception in Part 5 of the First Schedule and Division 2 under Part 2 of the Second Schedule of the amended Singapore DPDA, as discussed at paragraphs [2.36] to [2.44] of the Draft Advisory Guidelines On Key Provisions Of The Personal Data Protection (Amendment) Bill issued 20 November 2020 by the Personal Data Protection Commission (PDPC) of Singapore.

Yes. Both pro-privacy settings by default, and accessibility to pro-privacy settings for individuals with disabilities, should be required to the extent that it is reasonably commercially practicable for an APP entity to provide them.

4.10 Obtaining consent from children

33. *Should specific requirements be introduced in relation to how entities seek consent from children?*

The ACCC:

- "notes that digital platform users often include children who are likely to lack the capacity to understand how their personal information is collected, used and disclosed"; and
- is of the view "that consents to collect the personal information of children by APP entities must be obtained from the child's guardian".[39]

The UK Parliament's Joint Committee on Human Rights observed as follows:

> 34. Children and vulnerable adults are likely to find it particularly difficult to give meaningful consent, given the complexity of documents they are being asked to read. In addition, peer pressure to join the same social networks as their friends may make the 'take it or leave it' approach to consent especially problematic for children.
>
> 35. We do not believe that it is reasonable to expect 13 year-olds to give informed consent to their personal data being processed.[40]
>
> 36. We also believe there is a very strong likelihood of those under 13 regularly 'consenting' to their data being used, given that there is no meaningful way for a company to determine the age of the person consenting.
>
> 37. The general rule under Article 8 of the GDPR is an age of digital consent of 16. Protections for children in the UN Convention on the Rights of the Child should apply to all children under the age of 18. While the 'consent model' for data processing in the GDPR remains, the Government should urgently act to protect children by raising the age of digital consent to 16, and putting in place adequate protection for all those

[39] ACCC, Final Report of the Digital Platforms Inquiry, p 468

[40] In the UK a child aged 13 years or older can consent to their personal data being processed; parental consent is required to collect and process the information of children aged 12 and under. The US Children's Online Privacy Protection Rule ("COPPA") under the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505, imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. See further https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

> under 18 who access services online. In any case, consent should not be used as a basis for processing the data of children under the age of 16.[41]

A supportive approach is to create appropriate no-go zones to protect children (although query the appropriate age at which a child should become a young adult).

The Personal Data Protection Bill 2019 of India, as before the Lok Sabha, provides a good illustration of an overall principled approach. Clause 16 creates a specific no-go zone and appropriate carve-downs and targets the restriction at a subset of regulated entities, being any entity that the Authority, by regulation, classifies as a guardian data fiduciary because the entity operates a commercial website or online service directed at children or that processes large volumes of personal data of children.

Clause 16 reads:

> **16.** (1) Every data fiduciary shall process personal data of a child in such manner that protects the rights of, and is in the best interests of, the child.
> (2) The data fiduciary shall, before processing of any personal data of a child, verify his age and obtain the consent of his parent or guardian, in such manner as may be specified by regulations.
> (3) The manner for verification of the age of child under sub-section (2) shall be specified by regulations, taking into consideration—
> (a) the volume of personal data processed;
> (b) the proportion of such personal data likely to be that of child;
> (c) possibility of harm to child arising out of processing of personal data; and
> (d) such other factors as may be prescribed.
> (4) The Authority shall, by regulations, classify any data fiduciary, as guardian data fiduciary, who—
> (a) operate commercial websites or online services directed at children; or
> (b) process large volumes of personal data of children.
> (5) The guardian data fiduciary shall be barred from profiling, tracking or behaviouraly monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child.
> (6) The provisions of sub-section (5) shall apply in such modified form to the data fiduciary offering counselling or child protection services to a child, as the Authority may by regulations specify.
> (7) A guardian data fiduciary providing exclusive counselling or child protection services to a child shall not require to obtain the consent of parent or guardian of the child under sub-section (2).
> *Explanation.*—For the purposes of this section, the expression "guardian data fiduciary" means any data fiduciary classified as a guardian data fiduciary under sub-section (4).

[41] House of Commons & House of Lords, Joint Committee on Human Rights, 'The Right to Privacy (Article 8) and the Digital Revolution', HC 122, HL Paper 14, published on 3 November 2019, at paras [29]-[37]

4.11 The role of consent for IoT devices and emerging technologies

34. *How can the personal information of individuals be protected where IoT devices collect personal information from multiple individuals?*

An overarching "appropriate purpose" requirement is required: see sections 2 and 3 above of this submission.[42]

4.12 Inferred sensitive information

35. *Does the Act adequately protect sensitive information? If not, what safeguards should be put in place to protect against the misuse of sensitive information?*

Harm arising from excessive collection and misuse of sensitive information is a function of risk, likelihood and severity of impact upon individuals.

The current categories of sensitive information are only deemed sensitive because it was considered self-evident at the time of creating those categories that uncontrolled uses and sharing of information within those categories might lead to severe impacts upon individuals.

However, the risk and likelihood of uncontrolled uses and sharing of that information arising out of a particular activity are not best addressed through hard-coded categorisation of certain categories of personal information as sensitive information.

It is not practicable to endeavour to define all categories of sensitive information in a manner likely to be stable and effective to address new concerns as emerge over time.

For example, exact geolocation information has become sensitive information as a consequence of near ubiquitous use of smartphones.

Conversely, some types of health information might reasonably be contended to not be sensitive: for example, the data currently collected by a Fitbit™, is revealing as to activities and fitness status of a Fitbit user, but might not revealing of other aspects of an individual's health status.[43] Similarly, an APP 5 notice in relation to a medical consultation with a general practitioner that may involve pathology or other third party testing or referrals to a

[42] See also 'Beyond Data Privacy: Data Ownership and Regulation of Data Driven Businesses', Scitech Lawyer (American Bar Association), 16/2, Winter 2020 https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/winter/beyond-data-privacy-data-ownership-and-regulation-datadriven-business/

[43] See further Peter Leonard, 'Jobs Half Done: Getting Smart about Smartphones', UK Society for Computers and the Law Journal, October 2019 (https://www.scl.org/articles/10723-jobs-half-done-getting-smart-about-smartphones); Peter Leonard, 'Beyond Data Privacy: Data Ownership and Regulation of Data Driven Businesses', Scitech Lawyer (American Bar Association), 16/2, Winter 2020, https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/winter/beyond-data-privacy-data-ownership-and-regulation-datadriven-business/

specialist and associated exchanges of health information may be expected to be read by individuals that have some comprehension of the patient data ecosystem necessary to enable those activities to take place. Although 'personal information' that is 'health information' is 'sensitive information' and therefore subject to a higher expectations as to disclosure to an affected individual of relevant acts or practices (as well as required provision of consent), the form and level of disclosure could reasonably be tailored having regard to common understanding of customary medical practice and operation of legal duties of patient-doctor confidentiality.

Consideration should be given to amending the definition of "sensitive information" in section 6 of the Act s to include a new paragraph (f):

such other information or opinion about an individual as may be specified in the regulations for the purpose of this definition

or

such other information or opinion about an individual as the Australian Information Commissioner may by written direction specify as sensitive information for the purpose of this definition.

36. *Does the definition of 'collection' need updating to reflect that an entity could infer sensitive information?*

The act or practice of making an inference should of itself be regarded as a collection (through creation) of sensitive person information.

4.13 Overseas data flows and third party certification

48. *What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information?*

a. *Are APP 8 and section 16C still appropriately framed?*

Yes. This approach allows flexibility in cross-border disclosures while ensuring organisational accountability f the entity disclosing personal information to an overseas recipient.[44]

[44] See Peter G Leonard, Australian jurisdiction report, in Clarisse Girot et al (Asian Business Law Institute), Regulation of Cross-Border Transfers of Personal Data in Asia, Asian Business Law Institute, Singapore, 2019, https://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia. This publication also includes a detailed analysis of the national data privacy regulatory schemes in the Asian region, which enables evaluation of benefits and disadvantages of the respective national approaches. See also Dr Clarisse Girot and others, 'Data transfers after Schrems II: reflections from the Asia Pacific', Privacy Law and Business, forthcoming (as at December 2020).