Notice, Consent and Accountability:

addressing the balance between privacy self-management and organisational accountability

A paper for the Office of the Australian Information Commissioner

Peter G Leonard

June 2020

Table of Contents

Views of others

> *One of the most pervasive and persistent problems of privacy and data protection in the digital age is how to move the burden from consumers to read terms and conditions for services they are using, to the service providers to ensure they are clearly explaining the choices that consumers have, and the consequences for them.*

John Edwards, NZ Privacy Commissioner, *Click to consent? Not good enough anymore*[1]

> *The principle of consent has devolved from its role as a lynchpin of the privacy protective regulatory system a generation ago to a façade, which offers us today no more than the appearance and illusion of control over our personal information, while enabling in reality widespread corporate commercial data processing. Hastened along toward its demise by rapid technological development and new social and political paradigms of information sharing, the idea of consent, and the overarching principles of individual choice and control over personal information which it serves, can still be salvaged through a new regulatory approach. This approach should focus on the retention of consent in meaningful instances which have significant implications for individuals — such as the health-care, employment, and education contexts.*

Avner Levin (Professor and Director, Privacy and Cyber Crime Institute, Ryerson University), submission to the Office of the Privacy Commissioner of Canada's Consultation on Consent under PIPEDA[2]

> *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*

[1] Blog post on 2 September 2019, https://www.privacy.org.nz/blog/click-to-consent-not-good-enough-anymore/

[2] https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-consent-under-pipeda/submissions-received-for-the-consultation-on-consent/sub_consent_10/

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.

Report of the UK House of Commons and House of Lords, Joint Committee on Human Rights: The Right to Privacy (Article 8) and the Digital Revolution[3]

Our data protection laws have resulted in what Prof. Corien Prins and I have named 'mechanical proceduralism', whereby organizations go through the mechanics of notice and consent without any reflection on whether the relevant use of data is legitimate in the first place. In other words, the current preoccupation with what is legal is distracting us from asking what is legitimate to do with data. We even see this reflected in the highest EU court having to decide whether a pre-ticked box constitutes consent (surprise: it does not). Privacy legislation needs to regain its role of determining what is and what is not permissible. Instead of a legal system based on consent, we need to re-think the social contract for our digital society, by having the difficult discussion around where the red lines for data use should lie, rather than

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

passing the responsibility for a fair digital society to individuals to make choices they cannot fully comprehend.

Prof Lokke Moerel, EU Data Protection Laws Are Not Fit For Purpose: They Undermine the Very Autonomy of the Individuals They Set Out to Protect [4]

We are not going to have trustworthy systems, ethical processing or responsible data practices by requiring companies to leverage notice and consent. In a world of observation through billions of sensors, complex data flows, inferences and answers produced by sophisticated machine learning, and evolving business models and technology, meaningful consent prior to the use of data is near impossible. It's foolish to pretend otherwise and we're not persuaded by those who argue (disingenuously we believe) that we're not giving consumers credit for knowing what they want. Consent mechanisms can be easily manipulated, and they place the burden on individuals who are not equipped, even under the best circumstances, to make informed choices on the fly. We end up with false choices and pretty colors, not trustworthy business practices.

Marc Groman and Peter Cullen, Take the Long View: Demonstrable Accountability[5]

[4] Moerel, Lokke, EU Data Protection Laws Are Not Fit For Purpose: They Undermine the Very Autonomy of the Individuals They Set Out to Protect, Morrison & Foerster blog post 21 May 2020

[5] Marc Groman and Peter Cullen, Take the Long View: Demonstrable Accountability, Information Accountability Foundation blog post of 13 April 2020

Notice, Consent and Accountability: addressing the balance between privacy self-management and organisational accountability

A paper for the Office of the Australian Information Commissioner[6]

Peter Leonard[7]

PART A – SCOPE AND EXECTIVE SUMMARY

1 Scope

The Office of the Australian Information Commissioner (OAIC) commissioned Data Synergies to provide this paper. This paper:

- presents research on notice and consent, and how these privacy self-management tools might be re-balanced with organisational accountability practices in other privacy frameworks and in practice,
- presents analysis about the pros and cons of each approach to privacy self-management, and
- makes recommendations about:
    - ♦ potential models of notice, consent and organisational accountability that could be adopted in the Commonwealth privacy framework, and/or
    - ♦ further work that could be carried out on these issues.

[6] https://www.oaic.gov.au/. The writer gratefully acknowledges the contribution of comments and suggestions made by members of the OAIC team that reviewed drafts of this paper, including Sarah Croxall, David Moore and Rebecca Brown. However, the views expressed in this paper are those of the writer alone.

[7] Peter Leonard is a data, content and technology business consultant and lawyer advising data-driven business and government agencies. Peter is principal of Data Synergies and a Professor of Practice at UNSW Business School (IT Systems and Management, and Business and Taxation Law). Peter chairs the IoTAA's Data Access, Use and Privacy work stream, 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 of the NSW Data Analytics Centre. Peter was a founding partner of Gilbert + Tobin, now a large Australian law firm. Following his retirement as a partner in 2017 he continues to assist Gilbert + Tobin as a consultant.

2 Executive Summary

Most data privacy statutes enacted around the globe over the last four decades are based on a notice and consent framework for data protection, as implemented through privacy policies, privacy notices at collection and requests for consent.

However:

- Hardly anyone actually reads privacy policies or privacy notices at collection or requests for consent. Most people using small screen access devices routinely click-through 'I agree'.
- There is no convincing evidence that ever more prominent and plainly worded privacy notices at collection, or ever more granularly particularised requests for consent, will shift behaviour of most individuals towards more rigorous review of privacy policies, privacy notices at collection, or terms of consent. Nor is there convincing evidence to the contrary: we simply don't know. However, there is clear evidence of a continuing decline in digital trust of users of online services as to handling of personal information by many online businesses with whom they deal. Despite this decline in digital trust, there does not appear to have been a fundamental shift in consumer behaviour: most people still routinely click-through 'I agree'.

Given these factors, caution is warranted as to expectations that better and simpler information for individuals as to how personal information about them is handled by regulated entities will promote a fundamental shift in user behaviour towards adopting more privacy protective settings as may be offered to them.

In the last few years, many regulators and civil society organisations representing interests of individuals have deemphasised the need for legislative reforms to effect provision by related entities of better and simpler information for affected individuals, and considered further legislated restraints upon the circumstances in which personal information about individuals may be collected, used or disclosed, regardless of notice or consent.

Of course, it is also reasonable to ask:

- If most affected individuals will not fundamentally change their behaviour (i.e. will not slide their privacy settings towards more protective) following improvements in disclosures to them, doesn't this demonstrate that they don't care sufficiently to make the change?
- If so, why is a regulator forcing a change that most individuals don't care about?

This paper endeavours to squarely address those questions. However, part of the answer to those questions may be that individuals do not understand the nature or extent of harms that they may suffer as a result of unanticipated sharing and uses of data about them. A related paper is intended to be read in conjunction with this paper and addresses the

significance of 'privacy harms' and whether they are properly understood and managed by regulated entities and by affected individuals that may suffer these harms.

The current paper looks at a narrower issue: can the Australian Privacy Principles be revised to better address concerns as to:

- what is a *reasonable* collection, use or disclosure of personal information about an affected individual, and
- when is a collection, use or disclosure of personal information about an affected individual or notice *unfair* to an affected individual, regardless of what disclosures as to that act or practice have been made by an APP entity.

This paper and the related paper note that:

- *reasonableness* and *fairness* are related concepts, but distinct and different from existing protections within the APPs, including the existing requirement that collection must be only *by lawful and fair means*, and
- the concept of what is *unfair* is quite different from the concept of an *unreasonable intrusion upon an individual's right in and to data privacy.* Accordingly, extension of the consumer protection concept of unfair contract terms into the domain of data protection disclosures will not adequately address data privacy rights of affected individuals and protective privacy harms to individuals.

This paper examines what might reasonably be achieved through:

- legislative reforms to effect provision by related entities of better and simpler information for affected individuals – broadly, through innovations in the notice and consent framework to better empower affected individuals, and
- the closely related things that might be done (to promote rights and interests of affected individuals) outside of the notice and consent framework but still within the broad ambit of the Australian Privacy Principles.

Critiques of the notice and consent framework for data privacy regulation focus upon the 'illusion of consent', as described by Paul Ohm, Fred Cate and other privacy scholars, or its more recent restatement by Dan Solove and others as 'the privacy self-management problem'. These critiques juxtapose the many problems with privacy self-management (by the affected individual) against new measures as to organisational accountability (of the entity collecting, handling or disclosing personal information about the affected individual): that is, innovations in privacy regulation that are outside the notice and consent framework. These critiques are therefore important inputs into the discussion in this paper, and an important reality check upon expectations that regulatory innovations in the notice and consent framework will fundamentally shift behaviour of users.

A number of innovations for the notice and consent framework for data protection have been advocated over the last decade. Proposed changes included regulation to mandate:

- more prominent and plainly worded privacy notices at collection,
- standardisation of key privacy terms,
- granularly particularised requests for consent,
- addition of further acts or practices that require express user consent,
- layered privacy policies and privacy notices,
- just-in-time notices as to collection, and
- ongoing reminders as to privacy settings.

This paper makes a number of changes to Australian privacy regulation to promote such innovations, while cautioning as to their effectiveness, to substantially improve data privacy outcomes for consumers. Complementary initiatives outside the notice and consent framework are also required.

Over that same decade, and largely in response to building pressure from regulators around the globe, privacy disclosures by some regulated entities have significantly improved. Notable improvements have included through use of plain language, better structuring and heading of relevant paragraphs, deployment of more engaging and discoverable user interfaces (such as 'privacy centres'), and better clarity and specificity.

However, many other regulated entities, and including some global entities whose business is based upon capture of rich user data, continue to conduct their businesses behind impenetrably complex, convoluted and opaque user terms and privacy policies. Outside of the few global data platforms that are at the centre of attention of regulators, many regulated entities continue to operate with privacy disclosures tidied up and improved, but not fundamentally rewritten, over the last decade. Notice as to important but purportedly secondary uses and disclosures of personal information about users are often buried several layers, or many paragraphs, down. Some regulated entities purport to obtain consent as to significantly privacy affecting uses and disclosures of personal information, such as uses and disclosures of geo-location information, following disclosures to users that can only enable users to be properly informed, if at all, through multiple clicks and reading through multiple layers of text. Disclosures as to uses for profiling or other forms of individuation of affected individuals are often opaque or non-existent.

As this paper will demonstrate, it is now commonly accepted that there are shortcomings in specification of permitted notice and consent mechanisms under most data protection statutes in operation around the globe.

A fundamental dilemma of notice and consent is a choice between either making it simple and easy to understand or fully informing people about the consequences of giving up data, which are quite complex if explained in sufficient detail to be meaningful.

A further problem is that because consent is often bundled with notice, and terms of the notice not immediately adjacent to the 'I agree' "option", the separate concepts of notice and consent are conflated.

Specifically:

- The distinction between consent as required for a sub-set of categories of personal information, and notice only as required for other categories of personal information, is blurred.
- The distinction between what information must be stated:
    - ♦ in a form of consent (where consent is required),
    - ♦ in a notice at collection;
    - ♦ in a privacy policy,

  is not clear and often leads to repetition or complexity, and sometimes confusion and contradiction, rather than enabling efficient multi-layered communication through cross-referencing and more ready access to particular information that particular individuals might wish to read.
- The distinction between some acts and practices of handling of personal information, for which consent of the individuals required, and other acts and practices for which notice must be provided, is lost, with the result that description of and consenting to more impactful or unusual privacy affecting acts and practices is 'lost in the noise' of description of more generic, customary or expected, privacy affecting acts and practices.
- Many critics undervalue the benefits of notice (without consent), whether given through a privacy policy or a notice at collection, and then advocate 'beefing up' (1) the list of circumstances in which consent should be required, and (2) the requirements for an unambiguous, express, fully informed consent. Although this additional transparency may cause some APP entities to moderate more privacy invasive acts or practices, there is also a risk that such changes would prompt other APP entities to game a 'consent fatigued' individual, further reducing the utility of consent.

Regulatory design of requirements (and incentives and sanctions relating to) for:

- privacy policies,
- notices at collection, and

- forms of express consent, and presentation of information adjacent to seeking to consent, and
- measures for organisational accountability[8] and data risk and impact assessment, mitigation and management of residual risks,

need to be designed to take due account of current and likely continuing consumer behaviours and properly aligned with each other.

Current consumer behaviours in relation to requests for consent demonstrate continuing debasement of the currency of consent.

This paper contends that the value of consent will not be restored if we expand the myriad of circumstances in which consent is required.

The counter-view is that regulating to require increased granularity and prominence of requests for consent would have a valuable deterrent effect of causing a significant reduction in the number and range of acts and practices of regulated entities that are data privacy invasive.

This paper contends that although extending regulatory requirements to obtain consent should cause some reduction in the range and number of current privacy invasive acts and practices, that range and number is unlikely to reduce to a point where the volume of requests for consent become manageable for individuals. Until that point is reached, consent fatigue, and gaming by regulated entities of consent fatigue, are likely to remain characteristic features of online data 'privacy'. Accordingly, 'beefing up' consent of itself is unlikely to be an effective regulatory tool to reduce the range of current privacy invasive acts and practices to the point at which the volume of requests for consent become manageable for individuals.

In any event, there is a more urgent, current problem that has not been the subject of proper discussion in the privacy community. This paper contends that:

- consent of individuals is a valuable resource that should be carefully conserved for when it is really appropriate to be sought and obtained. As we move into a more automated and highly individuated world of personalised medicine and personalised offers and denials of offer of products or services enabled through data sharing and data linkage, we (Australian society, as a social good) need to *conserve requests for individual consent*

[8] As discussed in section 4 of this paper. See also Centre for Information Policy Leadership (CIPL), Organizational Accountability– Past, Present and Future, 30 October 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_organisational_accountability_%E2%80%93_past_present_and_future__30_october_2019_.pdf; e Margot E. Kaminski & Gianclaudio Malgieri, Algorithmic Impact Assessments Under the GDPR: Producing Multi-layered Explanations (Univ. of Colo. Law, Legal Studies Research Paper No. 19-28, 2019), https://ssrn.com/abstract=3456224;

for when consent is really needed (both as a social good, and as an important protection of an individual right in and to data privacy), and

- by expanding through regulation of *the range of circumstances in which consent must be obtained*, or the pre-conditions for a valid consent, legislatures and regulators run the risk of further debasing the currency of consent, just as effectively as the continuing erosion of value of consent caused by users continuing to blithely click through "I agree" to less opaque, more granular and prominent privacy notices at collection.

There is a further fundamental problem with our current consent framework. The categories of '*sensitive information*' for which consent must be obtained do not properly reflect the risks of significant privacy harms being caused to affected individuals from particular acts or practices of regulated entities through collection, handling and disclosure of personal information. Some acts and practices using non-sensitive personal information may be significantly more impactful than other acts or practices using sensitive information.

The options for reform of Australian privacy laws as set out in this paper reflect the analysis in this paper as summarised above.

This paper also suggests that many of the criticisms of notice and consent set up a false dichotomy between privacy self-management and organisational accountability.

This false dichotomy leads some critics of the notice and consent framework to over-emphasis the value of some advocated reforms *outside of the required form and substance of notice and consent*, such as:

- creation of *no-go zones* (being legislated specification of particular acts or practices for which consent cannot be obtained);
- introduction of *new tests as to objective reasonableness of acts and practices*; and
- extension of regulatory powers to prohibit *unfair acts or practices* (expanding current consumer law prohibitions as to unfair contract terms).

This paper advocates such reforms, while noting that there is already reasonable evidence from comparable economies (notably the European Union and Canada) suggesting that such reforms are unlikely to be effective to significantly improve privacy outcomes for affected individuals *without additional regulation to mandate demonstrable organisational accountability*.

This paper and the related paper contend that *privacy self-management and organisational accountability can and should be complementary regulatory requirements and designed to work together for a common objective of giving practical effect to a right of individuals to data privacy, while facilitating responsible operation of businesses in the modern digital economy*.

The notice and consent framework in the Privacy Act 1988 effects a measure of transparency as to acts and practices of APP entities. Transparency is a necessary, but insufficient, element to demonstrate organisational accountability. Some APP entities are unlikely to demonstrate accountability without an effective requirement of transparency through notice to affected individuals. Accordingly, transparency to affected individuals is a useful check on what APP entities may seek to do. Implementation of the recommendations made in this paper should dissuade some APP entities from some more privacy invasive acts and practices. However, the improvements in transparency recommended in this paper should not be considered in and of themselves as an effective control of data privacy, given:

- the pace of innovation and change in the modern digital economy,
- the increasing range, complexity and inter-relationship of interactions between humans and machines, and
- the corresponding richness, and therefore privacy invasiveness, of the data fuel and data exhaust of those interactions.

The Privacy Act 1988 does not currently include legal requirements for APP entities to implement organisational accountability, and to do through so demonstrated and reliable implementation of controls and safeguards. This lacuna is a fundamental deficiency in current Australian data privacy law.

Recommendation 1 (Bringing privacy rights and harms explicitly into the APPs) in section 4.3 of this paper, and the recommendations of the related paper on privacy harms, addresses possible reforms to effect a legislated requirement for APP entities to act reasonably to assess, mitigate and manage residual risks (remaining after proper mitigation) of significant privacy harms to affected individuals.

Recommendation 3 (Expanding permitted general situations and permitted general situations and creating a broader category of legitimate uses) in section 6.5 of this paper, and Recommendation 4 (Effecting privacy by default by, for example, aligning defaults with consumer preferences), are also recommended regardless of whether recommendations for specific reforms to the notice and consent framework (Recommendations 2 and 4 through 19) are considered for implementation.

We particularly highlight the need for a new and clear link between the current requirements of current APPs and a newly legislated requirement for APP entities to identify and mitigate significant privacy harms that their acts or practices in collection and handling of personal information may cause affected individuals. Without that link being clearly legislated, many privacy impact assessments are likely to continue to be formulaic applications of the APPs as criteria for drafting of notices and requests for consent, rather than a catalyst for APP entities to build processes and practices that are properly respectful of individuals' rights in and to data privacy. We contend that reforms to the notice and

consent framework (as suggested in this paper) are unlikely to significantly improve data privacy outcomes for individuals unless this link is also legislated. This link does not currently exist in the Privacy Act 1988.

Without this link, data privacy by design and default and responsible data minimisation are laudatory design principles consistent with good implementation of the Australian Privacy Principles, but not an essential element of the Australian Privacy Principles.

Without this link, the notice and consent framework and the new legislated requirements that this paper advocates for organisational accountability will not be properly complementary and work effectively together.

Accordingly, this paper concludes that:

- reforms to the notice and consent framework (as outlined in Recommendations 2 and 4 through 19 in this paper) are highly desirable,

but likely to be insufficient to significantly improve data privacy outcomes for individuals, unless

- Recommendation 1 (Bringing privacy rights and harms explicitly into the APPs) of this paper,
- the recommendations of the related paper on privacy harms,
- Recommendation 3 (Expanding permitted general situations and permitted general situations and creating a broader category of legitimate uses), and
- Recommendation 4 (Effecting privacy by default by, for example, aligning defaults with consumer preferences),

are also adopted.

PART B – WHEN *TOO MUCH TO CHOOSE* FROM BECOMES *NO REAL CHOICE*

3 The problem with 'choice'

3.1 *'I agree'* – but to what, exactly?

Over the past two decades, in the context of online services, and especially online services accessed through small screen access devices, 'consent' of individuals in relation to collection and handling of personal information about them has increasingly defaulted to bundled 'I agree' click-through following link to notice of terms of provision and use of service and notice of data privacy related terms.

In many cases, some data privacy related terms are embedded within long and complex statements of terms of provision and use of service, and other data privacy related terms are 'incorporated' by reference to a general privacy policy of a supplier business.

Because:

- terms of service (a unilateral, adhesion contract),
- a privacy policy (a regulatory requirement),
- a privacy notice at collection (a further and distinct regulatory requirement), and
- 'I agree' a purported acceptance by an affected individual of all of the above,

are bundled together, a number of detriments often arise.

Specifically:

- the distinction between consent (as required for a sub-set of categories of personal information), and notice only (as required for all categories of personal information), is blurred, and
- the distinction in presentation between information that is required to be stated:
    - ♦ to ensure that a consent (where required) is fully informed,
    - ♦ in a notice at collection;
    - ♦ in a privacy policy,

  is not clear. This leads to repetition or complexity, and sometimes confusion and contradiction, in disclosures. A better approach to enable efficient multi-layered communication through cross-referencing and more ready access to particular information that particular individuals might wish to read,

- the distinction between some acts and practices of handling of personal information, for which consent of the individuals required, and other acts and practices for which notice must be provided, is lost.

As a result, description of and consenting to more impactful or unusual privacy affecting acts and practices is 'lost in the noise' of description of more generic, customary or expected, privacy affecting acts and practices.

3.2 Good regulatory design for notice and consent

Regulatory design of requirements (and incentives and sanctions relating to) for:

- privacy policies,
- notices at collection,
- forms of express consent, and presentation of information adjacent to seeking to consent, and
- measures for organisational accountability[9] and data risk and impact assessment, mitigation and management of residual risks,

need to be designed to take due account of current and likely continuing consumer behaviours and properly aligned with each other.

3.3 Negative incentives through expanded consent requirements

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 therefore 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.

[9] As discussed in section 4 of this paper. See also Centre for Information Policy Leadership (CIPL), Organizational Accountability– Past, Present and Future, 30 October 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_organisational_accountability_%E2%80%93_past_present_and_future__30_october_2019_.pdf; Margot E. Kaminski & Gianclaudio Malgieri, Algorithmic Impact Assessments Under the GDPR: Producing Multi-layered Explanations (Univ. of Colo. Law, Legal Studies Research Paper No. 19-28, 2019), https://ssrn.com/abstract=3456224;

Imposition of "demonstrable accountability" requirements[10] upon data collectors and data users may be more likely to effect minimisation of collection and use of personal information about individuals than imposing a further burden upon affected individuals to determine whether to give or refuse consent.

For example, consider uses of pseudonymised data subject to appropriate controls and safeguards, as compared to consent-enabled uses of personal information about identifiable individuals.

If fair and responsible handling of pseudonymised data about individuals is reliably and verifiably implemented:

- following proper risk assessment and mitigation, and with proper management of residual risks as to uses and disclosures of outputs to effect outcomes,
- with proper controls and safeguards as to the pseudonymised data analytics environment, the outputs allowed out from that environment, the entities to whom those outputs are provided and the outcomes for which those outputs may be used,

then use of pseudonymised data derived from personal information about individuals (which currently does not require consent in Australia and many other advanced data privacy regulating jurisdictions) is more significantly reduce risks of privacy harms than a use of personal information about individuals enabled through notice and 'consent'.

3.4 Differential and adverse impact on smaller regulated entities of extension of requirements for consent

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 global social media platforms, search engines, cloud consumer services, online commerce sites.

This is partly because consumers perceive[11] that they are dependent upon such services and are therefore more likely to give consent to such providers than providers of perceived less essential services, such as disaggregated (niche or specialised) or local services.

---

[10] As summarised by Christopher Docksey "Keynote on Accountability At the 41st Conference of Data Protection and Privacy Commissioners 24 October 2019 in Tirana, Albania"; Marty Abrams in his IAF blog post "Demonstrable Accountability and People Beneficial Data Use" of 24 March 2020, Marc Groman and Peter Cullen, "Take the Long View: Demonstrable Accountability" IAF blog post of 13 April 2020; and Lynne Goldstein, "Bermuda Report on Information Accountability: Prepared by the Information Accountability Foundation for the Office of the Privacy Commissioner for Bermuda", 28 March 2020, all available at https://informationaccountability.org

[11] "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, since the cost of opting out is often too high. If, for instance, the choice is

The providers of these services can use their ability to obtain and create consents to advantage, as compared to providers of disaggregated (niche or specialised) or local services.

A 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.

3.5 Why do you expect me to read all this stuff?

Every reader of this paper will know that she or he, like the writer of this paper and virtually everyone else they know, hardly ever reads privacy policies or privacy notices at collection.[12]

That fact is why any regulatory redesign of the notice and consent framework should take existing user behaviour as a given for the currently foreseeable future and commence with due scepticism as to whether the problem can be fixed from within the paradigm of notice and consent.

To put it simply:

The key question is not whether the notice and consent framework is broken.

---

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

[12] Gindin, Susan E., "Nobody Reads Your Privacy Policy or Online Contract: Lessons Learned and Questions Raised by the FTC's Action against Sears", Northwestern Journal of Technology and Intellectual Property 1:8, 2009-2010; Schaub, Florian and Rebecca Balebako and Lorrie Faith Cranor, Designing Effective Privacy Notices and Controls, 21 IEEE Internet Computing 70 (2017); Karegar, Farzaneh, John Sören Pettersson and Simone Fischer-Hübner, The Dilemma of User Engagement in Privacy Notices: Effects of Interaction Modes and Habituation on User Attention, ACM Trans. Priv. Secur., Vol. 23, No. 1 (February 2020)

Instead, the key question is whether the broken framework is best fixed by working within that framework to remedy its defects.

As stated in a Report to President Obama by the President's Council of Advisors on Science and Technology:

> Notice and consent is, today, the most widely used strategy for protecting consumer privacy. When the user downloads a new app to his or her mobile device, or when he or she creates an account for a web service, a notice is displayed, to which the user must positively indicate consent before using the app or service. In some fantasy world, users actually read these notices, understand their legal implications (consulting their attorneys if necessary), negotiate with other providers of similar services to get better privacy treatment, and only then click to indicate their consent. Reality is different.
>
> Notice and consent fundamentally places the burden of privacy protection on the individual – exactly the opposite of what is usually meant by a "right." Worse yet, if it is hidden in such a notice that the provider has the right to share personal data, the user normally does not get any notice from the next company, much less the opportunity to consent, even though use of the data may be different. Furthermore, if the provider changes its privacy notice for the worse, the user is typically not notified in a useful way.
>
> As a useful policy tool, notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data. It is simply too complicated for the individual to make fine-grained choices for every new situation or app. Nevertheless, since notice and consent is so deeply rooted in current practice, some exploration of how its usefulness might be extended seems warranted.
>
> One way to view the problem with notice and consent is that it creates a non-level playing field in the implicit privacy negotiation between provider and user. The provider offers a complex take-it-or-leave-it set of terms, backed by a lot of legal firepower, while the user, in practice, allocates only a few seconds of mental effort to evaluating the offer, since acceptance is needed to complete the transaction that was the user's purpose, and since the terms are typically difficult to comprehend quickly. This is a kind of market failure.[13]

The "fundamental dilemma of notice" is a choice between either:

- "making it [the notice] simple and easy to understand", or

[13] President's Council of Advisors on Science and Technology [to the Obama Administration], Report to The President, Big Data and Privacy: Technological Perspective, May 2014; p38, see also pp xi-xii

- "fully informing people about the consequences of giving up data, which are quite complex if explained in sufficient detail to be meaningful."[14]

3.6 Thinking more carefully about what goes where

In trying to improve transparency to affected individuals, it is important to think carefully about the respective roles of a published privacy policy and a notice to individual at collection.

(A caution as to the following discussion: the views expressed in the next two pages of this paper does not reflect the traditional regulatory policy view of the respective roles of a privacy policy and a notice to individual at collection, and might be regarded by some privacy professionals as heresy.)

A privacy policy and a notice to individual at collection may be contended to have different goals which will often be in tension with each other:

> "The tension between these goals arises because many non-expert individuals can only comprehend and digest short and simple privacy notices. Such brevity and simplicity will often omit the details that regulators, policymakers, and experts need to evaluate what the organization is doing."[15]

A privacy policy should clearly, conspicuously, and accurately explain what a regulated entity is doing, and will not do with personal information about individuals and *provide sufficient information for regulated entities to be accountable to regulators, policymakers, and experts such as civil society organisations tasked with privacy advocacy and consumer protection*.

This statement as to intended acts and practices should then ensure that, through operation of data privacy laws and consumer protection laws, including through operation of statutory provisions addressing unfair contract terms and prohibiting the making of statements that are misleading or deceptive and unconscionable conduct, regulated entities can be held to account as to the gap between what the policy says they will do, and will not do, and what they do in practice.

In this respect, whether an affected individual elects to read a privacy policy may not be a reasonable indication of the value of a privacy policy.

Instead, the value of data privacy statements may better be judged by the behavioural constraints that such statements may impose upon regulated entities, such as through:

[14] Solove, Privacy Self-Management, op cit, at 1992
[15] Solove, Daniel J. and Schwartz, Paul M. op cit, at p16

- transparency and enduring, ready, availability data privacy statements for legal review ('*sunlight is the best disinfectant*'[16]),
- the process of evaluation by the regulated entity of what to say in its published privacy statements acting as a trigger to cause a regulated entity to conduct a privacy impact assessment and then moderate the privacy impact of its proposed acts and practices,
- the requirements of change control, and the process of evaluation of how to explain proposed changes (including to individuals in relation to whom personal information has already been collected under a preceding form of notice), acting as a trigger to cause a regulated entity to moderate the privacy impact of a proposed change in its proposed acts and practices.

By contrast to the content of a privacy policy, a notice at collection should explain to individuals how personal information about them is collected, used and disclosed (shared).

A notice at collection, by its nature, is directed to an affected individual in relation to a particular acts or practices *that are likely to be of direct relevance to an individual, and therefore (it is contended) should be intended to be read by the individual*.

This unavoidable (because it is reality) constraint should determine the focus, length and complexity of a notice at collection.

But the notice must also not be misleading through omission of key acts or practices addressed in the privacy policy or effectively contracted by statements made in the privacy policy.

Of course, this creates a narrow path for a regulated entity to follow, requiring subjective assessments by drafters as to which particular acts or practices are sufficiently likely to be of direct relevance to an individual to warrant summary in the notice at collection, while still ensuring that the notice is focussed and readily understood.

Given the difficulty and subjectivity of this assessment and balancing, a reasonable degree of latitude should be allowed to regulated entities.

A condition of that latitude should be that regulated entities ensure that notices are *properly targeted to prominently state more privacy affecting or likely unexpected acts or practices*.

Further, the difficulty of getting this disclosure path 'right' should prompt regulatory design thinking about alternative paths that might be opened up to address less privacy affecting or

[16] Attributed to leading U.S. jurist Louis Brandeis (1914), "What Publicity Can Do", in Other People's Money and How the Bankers Use It: "Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman." Available at http://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/other-peoples-money-chapter-v.

commonly expected acts or practices. This is why 'legitimate interests'[17] or like alternative avenues have an important role to play in making notice and consent work more effectively. Transparency is good, but not if an affected individual cannot see the wood for the trees.

And of course, 'legitimate interest' should only be opened as an alternative path if that path is opened at the cost of undermining reasonable expectations of data privacy.

Rather, legitimate interest should be used to 'reduce the noise' of disclosures and to potentially improve outcomes for individuals by concentrating their attention on enhanced and more prominent notice of more privacy affecting, or unexpected, acts or practices.

Given this analysis, analogies between privacy notices at collection and summaries of key terms in consumer contracts should be treated with caution. With that caution, it is noted that summaries for consumers of key terms are required under a number of Australian statutes. Examples include:

- telecommunications carriage service providers must provide to consumers 'critical information summaries' derived from detailed terms and conditions of a standard form of agreement[18],
- credit providers must provide "Key Facts Sheets" in relation to a range of credit products[19],

[17] Article 6(1)(f) of the GDPR states: "1.Processing shall be lawful only if and to the extent that at least one of the following applies: …(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." ICO UK suggest that this is a three part test to be applied in the following order: "Purpose test – is there a legitimate interest behind the processing? Necessity test – is the processing necessary for that purpose? Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms? See further ICO UK, What is the 'legitimate interests' basis? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

[18] See Australian Communications and Media Authority, Critical Information Summaries, at https://www.acma.gov.au/critical-information-summaries; C628:2019 Telecommunications Consumer Protections Code, Rule 4.2 (Critical Information Summary) at pp29-29, available at https://www.commsalliance.com.au/__data/assets/pdf_file/0011/64784/TCP-C628_2019.pdf.

[19] National Consumer Credit Protection Act 2009 (Cth), including at s133AC(2); s133BC(1); ; see the useful discussion in section 5.6.4 (page 43) of Jeannie Marie Paterson and Nicola Howell, Everyday Consumer Credit: Overview of Australian Law Regulating Consumer Home Loans, Credit Cards and Car Loans, Background Paper 4 to the Royal Commission into Misconduct in the Banking, Superannuation and Financial Service Industry, available at https://financialservices.royalcommission.gov.au/publications/Documents/australian-consumer-credit-protection-law-overview-background-paper-4.pdf

- energy retailers must provide a one page summary of their offer (an Energy Price Fact Sheet and written product disclosure statement), as well as "fair contracts with clear terms and conditions so you can fully understand the energy offer".[20]

It is suggested that all of the categories of information that APP 5 requires to be included in a privacy notice cannot reasonably be expected to be read by consumers, however carefully and well-structured a notice is drafted for a regulated entity.

APP 5 as currently drafted sets up APP entities to fail.

A layered notice may address some of the information overload, but once a notice at collection starts to be layered a reasonable question should arises as to whether the lower layers should be in the notice itself.

Further, 'hard coding' of the categories of information that must be addressed in a privacy notice, and those categories of information that is sensitive information for which consent is required, may also not be good regulatory design.

Firstly, the harm arising from a misuse of sensitive information is a function of risk, likelihood and severity of impact. The current categories of sensitive information are only deemed sensitive because it is self-evident 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 addressed in the hard-coded categorisation of a type of information as sensitive information.

Consider the following examples.

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 specialist and associated exchanges of health information may be expected to be read by individuals that have a reasonable 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.

[20] National Energy Retail Law and National Energy Retail Rules (Part 2 Customer retail contracts) as available at https://www.aemc.gov.au/regulation/energy-rules/national-energy-retail-rules/current, see also Australian Energy Retailer, Your energy rights, at https://www.aer.gov.au/consumers/choosing-an-energy-retailer/your-energy-rights

By contrast, many activities in the online advertising data ecosystem involve secondary uses or disclosures of information which may be personal information in the hands of some participants in that data ecosystem. Some of these participants may have no immediate connection to the nature of the affected individual's online activity. Their involvement and activities may be wholly outside the reasonable contemplation of the affected individuals. Because the handling of information relating to online activities of participants is by entities that have no direct relationship with the affected individual, those activities might reasonably be considered more 'sensitive' than handling of more sensitive information by entities known to an affected individual. Further, smartphones and other highly personalised devices, AI and predictive data analytics in many applications break the current regulatory paradigm that the specified categories of 'sensitive (personal) information' require a higher level of regulation because the potential harms as may arise through their handling (or mishandling) are greater (because sensitive information is more revealing about an individual's self).[21] Although sensitivity of (for example) information about an individual's search and purchasing activities might reasonably be regarded as significantly less than health information, in the case of adtech:

- the opaqueness of the relevant acts and practices, and
- the relationship distance between the affected individual and the adtech participant,

might be considered to warrant more prominent and fulsome notices at collection by the regulated entity first collecting the relevant information.

It is therefore difficult to generalise as to the key or essential information that might be required to be included in a notice at collection. Mandated key terms from the telecommunications, energy and credit provider sectors show significant diversity in specification of key terms. The medical practice sector provides an example where key terms are often inferred and not the subject of unambiguous express consent by patients.

A better regulatory design for determining those matters that require the additional controls of heighted notice and fully informed consent might be consideration of:

- the nature of the product, service or other act or practice that is the subject of the notice,
- the level of understanding that consumers might reasonably be expected to have of 'normal' or 'customary' data collection and handling practices associated with that activity, and

[21] See further Peter Leonard, 'Jobs Half Done: Getting Smart about Smartphones', Computers and Law (UK Society for Computers and the Law), December 2019; Peter Leonard, 'Data Ownership and the Regulation of Data Driven Businesses', Scitech Lawyer (American Bar Association), 16/2, Winter 2020

- the likely audience or segment of affected individuals,
- risk, likelihood and severity of impact upon affected individuals of the described act or practice,
- risk, likelihood and severity of impact upon affected individuals of the relevant personal information becoming available outside the controls and safeguards that the regulated entity puts in place to protect the described act or practice.

3.7 Other criticisms of the notice and consent framework

In a recent paper, Professor Daniel Susser[22] summarises more frequent criticisms of the notice and consent framework. These criticisms are often grouped under the rubric of 'illusion of consent', as described by Professor Paul Ohm, Fred Cate and other privacy scholars, or 'the privacy self-management problem' as more recently restated by Professor Dan Solove and others.[23]

I summarise Professor Susser's presentation of "five main criticisms" as below. It should be noted that many of these criticisms are reflected in the detailed analysis and findings of the ACCC in its Digital Platforms Inquiry Final Report.[24]

First, notice and consent typically fails to offer options for online service users that users regard as real options. The decision is *typically all-or-nothing*: accept the terms and conditions set forth in the terms of service or end-user license agreement (and linked privacy terms), or do not engage with the product or service at all.

Second, even when an entity provides users with real options, users often do not assess the options or use them. Consent becomes a tool for *legitimisation* of a laundry list of stated practices, *rather than a constraint* on those practices or an effective lever for narrowing of uses to reasonable and fair purposes.

Professor Susser also notes Daniel Solove's contention[25] that even if the average user could understand the average privacy policy, the user would face a variety of *common decision-making problems*. "Bounded rationality issues, such as availability heuristics and framing

[22] 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
[23] See the papers cited the end of this paper. Many authors converge in these criticisms, and, as Professor Susser acknowledges, the current statement of the criticisms represents a cumulation of analyses by respective authors.
[24] See in particular Chapter 7, Digital platforms and consumers in ACCC, Final Report of the Digital Platforms Inquiry, 2019
[25] Solove, Daniel J. "Privacy Self-Management and the Consent Dilemma." Harvard Law Review 126 (2013): 1880–903

effects, make it exceedingly difficult for individuals to weigh the costs of particular data practices against their own privacy interests."[26]

Professor Susser continues:

> "The third problem is that *notice-and-consent simply does not scale*. Most of us engage with a huge number of information actors—commercial websites and apps, government agencies, educational institutions, and so on. While we might be expected to read, understand, and evaluate a few of their privacy policies, it is inconceivable that we could keep up with them all.
>
> ……..
>
> The fourth criticism of notice-and-consent is what Daniel Solove describes as "*the problem of aggregation*". Things about us which do not seem particularly sensitive can, in the aggregate, reveal deeply personal information: the sum of data about us is greater than its parts. When individuals weigh the costs and benefits of disclosing particular pieces of information, they can't know what other information it will be combined with down the road. Notice-and-consent thus demands that we make onetime decisions that can have cascading effects, and we are in principle unable to predict those effects at the moment of decision."[27]

Fifth, data privacy regulation should protect both individual interests and social or collective interests. As Professor Helen Nissenbaum argues, privacy is a set of social norms, not a set of individual decisions. Privacy norms "preserve the integrity of the social contexts in which we live our lives, and they support and promote the ends, purposes, and values around which these contexts are oriented". [28]

3.8 What notice and consent cannot address

The routine clicking through of 'I agree' is particularly problematic.

In some cases, 'I agree' may reasonably signify a valid informed consent, even if bundled.

For example, most individuals routinely 'accept' without charge ('free', but paid for through personal information) provision of an advertising funded online service applying an intuitive understanding as to the deal. The deal is a bargain of extraction of personal information about an individual in consideration of not being required to pay for the service.

[26] Susser, op cit, at p44, citing Hanna, Jason, ''Consent and the Problem of Framing Effects", Ethical Theory and Moral Practice, 1, no 5 (2011), pp 517-31.
[27] Susser, op cit, at p44
[28] Nissenbaum, Helen, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford, CA, Stanford Law Books, 2010, at p 186

This intuition might or might not be properly informed if the individual elected (as most individuals do not do) to read such privacy disclosures as are proffered to them by a regulated entity.

In many cases, that intuition will correctly reflect the reality of some privacy affecting uses and disclosures as detailed in those privacy disclosures, but not other uses or disclosures as detailed in those privacy disclosures and that may cause significant and unexpected detriments to some affected individuals.

These detriments may be through unexpected and excessive collection and sharing of personal information: for example, the flashlight app that collects and passes to others geo-location data about an individual using the app, even though it is not used by the app in any way.[29]

In some cases, significant and unexpected detriments to some affected individuals may arise regardless of whether a regulated entity intends for those detriments to arise.

A media content publisher may derive revenue from third party targeted advertising carried in widgets or banners on the media site and directed to users of their media content. The publisher may expect that use of online tracking code that it makes available to an advertising services provider is properly managed and controlled within an advertising data ecosystem that operates outside effective control of the media content publisher. That expectation of management and control by others may be incorrect.[30]

An at-risk individual may 'agree' to use an app, not understanding that the app may be legally accessed by a person who is a would-be causer of harm to that individual, and provide information that materially increases the risks to safety of the affected individual through that prospective access by a motivated third party. The regulated entity may or may not disclose that risk to the at-risk individual, by prominent notice or otherwise. As many data privacy laws currently stand, this risk of significant harm (caused by a third party not under the control or direction of the regulated entity) is not required to be disclosed by a regulated entity to a potentially affected individual. The at-risk individual might not elect to provide that information if the individual had understood this risk.[31]

An individual may 'agree' to provision of personal information about the individual without understanding that this information may be processed and de-identified and then used to

[29] A free flashlight app might reasonably collect and use geo-location information for geo-targeted advertising directed to a user, if that geotargeting of ads is properly disclosed and controlled.
[30] See further materials of the UK Centre for Data Ethics and Innovation (CDEI) Review of online targeting, as available at https://www.gov.uk/government/publications/cdei-review-of-online-targeting.
[31] For examples, see UK CDEI Snapshot Paper - Smart Speakers and Voice Assistants, available at https://www.gov.uk/government/publications/cdei-publishes-its-first-series-of-three-snapshot-papers-ethical-issues-in-ai

deliver differentiated outcomes to that individual. For example, deidentified information may be used in conjunction with online audience segments to enable individuation of offers, pricing for offers, demands for payments or other calls to action that an affected individual does not understand and which may lead to significant adverse individuated effects upon that individual.[32]

An individual may 'agree' to provision of personal information about the individual without also understanding that this information is potentially accessible by a myriad of third parties as "required or authorised by law". That individual might not elect to provide that information if the individual had understood this risk.

In other words, the intuitive understanding of affected individuals of what a regulated entity does, or what a product or service is, is often not a reliable guide to their anticipation or expectation of collections and uses and disclosures of personal information about them.

3.9 Improving notice and consent through incentives and constraints

The *user choice* underpinning of a notice and consent framework is therefore problematic unless:

- coupled with *incentives to* or *constraints upon* entities collecting, using or disclosing personal information, and
- those incentives or constraints operate to ensure outcomes which are not reasonable having regard to the extent and impact of the activities of the regulated entities upon data privacy rights of affected individuals.

Some individuals may value data privacy rights more highly than others.

Some individuals may not care at all about their right of data privacy.

A notice and consent framework should enable choice by those users that do wish to make an informed choice.

However, that framework should not put a reasonable expectation of data privacy at jeopardy if a user is unable or unwilling to make the significant effort that is now required to inform a choice by an affected individual as to significantly data privacy affecting collections, uses and disclosures of personal information in the course of provision of a complex product or service offering.

And most products or services, however simple in their user interface and presentation, are now complex in relation to collections, uses and disclosures of personal information. This

[32] See further CDEI blog post on 14 May 2020, Public attitudes on the fair use of data and algorithms in finance, https://cdei.blog.gov.uk/2020/05/14/public-attitudes-on-the-fair-use-of-data-and-algorithms-in-finance-collaborating-with-the-behavioural-insights-team-bit/

complexity arises because offer and provision of many products or services, offline as well as online, involves complex multi-party data ecosystems and is at least partially fuelled by personal information about individuals.

Important constraints upon significantly data privacy affecting acts and practices of entities arise through operation of consumer protection laws. It is not surprising that regulatory responses in many jurisdictions to significantly data privacy affecting acts and practices of entities have been framed in contract law and U.S. law as to fair consumer practices, given:

- the prevailing, almost ubiquitous, 'I agree' paradigm,
- the fact that most relevant data interactions between individuals and regulated entities are in the context of consumer contracts,
- the influence of Californian based global digital businesses, and
- the global business law influence of United States jurisprudence.

Consumers have become familiar with U.S. consumer contract models as adopted by Californian based global digital businesses in provision of free or freemium online services and electronic commerce sites. Of course, the most common U.S. consumer contract model for online services was, and remains, bundled 'I agree' click-through, without significant 'just-in-time' information at collection and instead with link to lengthy terms of provision and use of service and a privacy policy.

Because the U.S.A. failed to enact economy-wide consumer data privacy laws, the U.S. Federal Trade Commission, as the principal consumer protection regulator in the U.S.A., has sought to seek to protect consumers' legitimate expectations of data privacy through exercise of the FTC's jurisdiction to prosecute misleading and deceptive trade practices.[33] The FTC has been quite effective in exercise of this statutory authority to extract after-the-event penalties and undertakings from U.S. based entities to address more egregious misleading uses and disclosures of personal information of individuals. However, exercise of this jurisdiction has not precluded outcomes which are unreasonable having regard to the extent and impact of the activities of the regulated entities upon data privacy rights of affected individuals. As a result, there is increasing pressure for statutory protection of data privacy of individuals through both State and Federal statutes, including the Californian Consumer Privacy Protection Act of 2018.

[33] Under Section 5(b) of the FTC Act, the Commission may challenge "unfair or deceptive act[s] or practice[s]," "unfair methods of competition," or violations of other laws enforced through the FTC Act, by instituting an administrative adjudication. For a useful summary, see Federal Trade Commission, A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority, Revised October 2019, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority

In parallel, U.S. businesses, including the Californian based global digital businesses, responded to this regulatory action by the FTC with ever more fulsome descriptions of data practices. Often this more fulsome description is now there, somewhere, in the terms as read by virtually no-one.

Increasing length and complexity of terms has further obscured consumer understanding of less expected, or higher risk or impact, data practices, including data sharing with third parties.

Where separate 'privacy centers' or other mechanisms are offered to consumers that might wish to change privacy settings, this optionality is often substantially uncoupled from the notice of terms of provision and use of service and notice of data privacy related terms. Consumers are informed that they could go to other areas of a provider's website to select and change data privacy related settings. Most consumers take the readily available option, click-through 'I agree' to 'accept' default settings, and do not later change these default settings.

The net effect is that the form of notice (a legal offer), wrapped with a click through consent (a legal acceptance), creates a legal illusion of voluntary contract between provider and consumer, in circumstances where the consumer often had not turned their minds at all to the subject matter of the data consent. Notice and consent are conflated and confused.

However, it should also be noted that the fair information principles as developed by the Federal Trade Commission state *notice* and *choice* (note: *choice*, not *consent*) as separate and distinct requirements.

The FTC's statement of fair information principles for online services recommends that entities collecting user information:

> 1. *Notice*: provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through nonobvious means such as cookies), how they use it, how they provide choice, access, and security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.
>
> 2. *Choice*: offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as

marketing back to consumers) and external secondary uses (such as disclosing data to other entities).[34]

In practice, the notice and *consent* framework does not create the preconditions for an informed *choice* by affected individuals that the FTC intends businesses to make available to them.

3.10 The complementary role for Australian Consumer Law

Australian consumer law is better placed than U.S. federal law to address more egregious or hidden[35] data privacy affecting acts or practices.

The specific Australian prohibition on misleading and deceptive conduct is found in section 18 of the Australian Consumer Law (**ACL**) (Schedule 2 of the Competition and Consumer Law Act 2010 (C'th)). This prohibition was initially modelled on what is now section 5(1) of the Federal Trade Commission Act (**FTC Act**).

Section 18 states that "a person must not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive". The terms "misleading" and "deceptive" are not defined in the ACL, so the dictionary meaning of both words has been generally adopted. A court must determine whether conduct is misleading or deceptive as a question of fact in the context of the whole transaction. The focus is on whether the conduct is "likely" to mislead actual deception or loss or damage to the consumer is not required. This is similar to the position in the U.S.A., where a company does not need to 'intend' for conduct to be misleading and deceptive for it to be found to be so. However, arguably section 5(1) of the FTC Act only gives the FTC authority to investigate a higher threshold of "unfair and deceptive acts and practices in or affecting commerce". There is no requirement of "unfairness" in Australia.

Section 21 of the ACL currently prohibits conduct in connection with an actual or potential transaction "that is, in all the circumstances, unconscionable". This is a moral standard based on community expectations, taking into account a number of non-exhaustive statutory factors set out in section 22 of the ACL. However, the provision has proven in the courts to be of limited utility to protect vulnerable persons.[36]

[34] U.S. Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress, May 2000

[35] See further Kemp, Katharine, "Concealed Data Practices and Competition Law: Why Privacy Matters" [2019] UNSWLRS 53, available at http://www.austlii.edu.au/au/journals/UNSWLRS/2019/53.html

[36] See for example Australian Securities and Investments Commission v Kobelt [2019] HCA 18.

Terms in standard form consumer contracts[37] are regulated by the ACL unfair contract terms (**UCT**) provisions.[38] A term of a consumer contract is unfair if it:

- would cause a significant imbalance in the parties' rights and obligations arising under the contract,
- is not reasonably necessary to protect the legitimate interests of the party who would be advantaged by the term; and
- would cause detriment (whether financial or otherwise) to a party if it were to be applied or relied on.[39]

A number of factors are required to be taken into account when deciding whether a term is potentially unfair. The fairness of a term must be considered in the context of the contract as a whole. In determining whether a term of a standard form consumer contract is unfair, a court may consider any matter that it thinks relevant. It must take into consideration the extent to which the term is transparent, and the contract as a whole. A transparent term in a standard form consumer contract may cause a significant imbalance in the parties' rights and obligations. A term is considered to be transparent if it is expressed in reasonably plain language, legible, presented clearly, and readily available to any party affected by the term. Terms that may not be considered transparent include terms that are hidden in fine print or schedules, phrased in legalese or in complex or technical language, or that are ambiguous or contradictory.

The constraints that the ACL UCT provisions impose upon significantly data privacy affecting collections, uses and disclosures of personal information by Australian businesses are limited in a number of ways.

First, the unfair contract terms provisions only apply if there is a standard form consumer contract. A privacy policy, and a notice at collection, is a document required by statute, but may not be a contract. In its Final Report of the Digital Platforms Inquiry, the ACCC noted that it considers privacy policies to be standard form contracts, and that due to the significant information asymmetries and bargaining power imbalance in the relationship between consumers and digital platforms, consumers are unable to negotiate terms relating to the collection, use and disclosure of personal data.[40] This bargaining imbalance therefore results in potentially unfair contract terms under the ACL. The ACCC does not the legal basis

[37] ACL section 23(3)
[38] ACL section 24. See further ACCC, Unfair contract terms, A Guide For Businesses And Legal Practitioners, 2016, https://consumerlaw.gov.au/sites/consumer/files/2016/05/0553FT_ACL-guides_ContractTerms_web.pdf; Peter Sise, The Unfair Contract Term Provisions: What's Transparency Got To Do With It?, QUT Law Review, 17 (1), October 2017, pp 160–173
[39] ACL section 24(1)
[40] Ibid, section 7.4 The nature of consumer consents

for its view that a privacy policy (whether unilaterally presented as 'terms' or not) to be a contract. The ACCC's view is legally contentious.

The ACCC also highlighted particular concerns regarding the collection, use and disclosure of personal information by businesses operating on digital platforms. "The existing Australian regulatory framework for the collection, use and disclosure of user data and personal information does not effectively deter certain data practices that exploit the information asymmetries and bargaining power imbalances between digital platforms and consumers".[41]

The ACCC also recommended that entities should be deterred from engaging in certain data practices that cause significant consumer detriment by introducing a prohibition on certain unfair trading practices to effectively regulate problematic conduct that is not currently expressly prohibited under the ACL. The Commission:

> ….identified some kinds of conduct that it considers to be significantly detrimental to consumers which are not expressly prohibited by the ACL. Such conduct includes:
>
> - businesses collecting and/or disclosing consumer data without express informed consent
> - businesses failing to comply with reasonable data security standards, including failing to put in place appropriate security measures to protect consumer data
> - businesses unilaterally changing the terms on which goods or service are provided to consumers without reasonable notice, and without the ability for the consumer to consider the new terms, including in relation to subscription products and contracts that automatically renew
> - businesses inducing consumer consent or agreement to data collection and use by relying on long and complex contracts, or all or nothing click wrap consents, and providing insufficient time or information that would enable consumers to properly consider the contract terms
> - business practices that seek to dissuade consumers from exercising their contractual or other legal rights, including requiring the provision of unnecessary information in order to access benefits.[42]

Secondly, the unfair contract terms provisions apply in relation to consumer contracts. Many privacy affecting acts and practices occur within supply side data ecosystems where the entity engaging in the act or practice is not directly in a consumer transaction relationship with a consumer.

[41] Ibid, page 374, see further section 7.10.
[42] Ibid., Recommendation 21 – Prohibition against certain unfair trading practices, pages 498-501.

Thirdly, unfairness or otherwise is determined by factors including whether the act or practice is addressed in a term which if given effect would cause a significant imbalance in the parties' rights and obligations arising under the contract.[43] An individual's right in and to data privacy under the Privacy Act 1988 only roses if and to the extent that the right arises, relevantly, by being contrary to the Australian Privacy Principles. In relation to many acts and practices that significantly affect data privacy interests of individuals, the Australian Privacy Principles do not clearly create relevant enforceable 'rights' of affected individuals.

Fourthly, a definitional issue will often arise as to whether a contractual permission (if that is what it is) created through valid notice or consent provided in accordance with the Privacy Act 1988 and addressing a privacy affecting act or practice *causes* a significant imbalance in the parties' rights and obligations, or if this imbalance *aris[es] under the contract.*

Fifthly, many significantly privacy affecting provisions in privacy policies or privacy notices are manifestly not transparent, but a term that is not transparent will not necessarily be unfair. (Conversely, transparency alone will not necessarily overcome underlying unfairness in a contract term.)

Lastly, enforcement of the UCT provisions is complex and expensive. The best resourced and experienced litigator of these provisions, the ACCC, has been unsuccessful in some prosecutions based upon the provisions. The provisions do not create predictably available and practically enforceable remedies for individuals.

The ACCC has enumerated other concerns concerning the unfair contract terms provisions. As the ACCC puts it, "general deterrence in an industry is difficult to achieve under the current UCT regime.[44]

As at May 2020, the Federal Government is considering submissions made in consultations about the introduction of penalties for the use of unfair contract terms.[45] Currently, there are no penalties.[46] If penalties are introduced, entities will want as much guidance as possible about whether a particular term is unfair. Unfortunately, since the context of a

[43] ACL section 24(1). See further Manwaring, Kayleen, 'Will Emerging Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation' (September 1, 2018); Manwaring, Kayleen, 'Emerging Information Technologies: Challenges for Consumers' (April 25, 2017); and Kemp, Katharine, 'Concealed Data Practices and Competition Law: Why Privacy Matters', [2019] UNSWLRS 53

[44] ACCC Submission to Review of Unfair Contract Term Protections for Small Business, 21 December 2018. See also "Fair shake: Prohibiting unfair practices in Australia", blog post by Gilbert + Tobin Lawyers, 21 November 2019, https://www.gtlaw.com.au/insights/fair-shake-prohibiting-unfair-practices-australia

[45] See further Australian Treasury, Enhancements to Unfair Contract Term Protections, Consultation Regulation Impact Statement, December 2019

[46] As Recommendation 20 of the Final Report of the Digital Platforms Inquiry, the ACCC recommended that the ACL be amended to introduce a prohibition on the use of unfair contract terms in standard form consumer or small business contracts. The prohibition would be backed up by penalties that apply to breaches of the new provisions.

contract is important to whether a term is unfair, judgments on whether a particular term is unfair are of limited assistance.

In summary, the UCT provisions, the prohibition on misleading and deceptive conduct, and the prohibition of unconscionable conduct in connection with an actual or potential transaction, do not fill the gap between the protections currently afforded to affected individuals by the Privacy Act 1988 and acts and practices of entities collecting, using and disclosing personal information to create outcomes which are unreasonable having regard to their impact upon data privacy rights of affected individuals.

So how do we identify, and then address through new regulation, outcomes which are unreasonable having regard to their impact upon data privacy 'rights' of affected individuals?

Part C of this paper address that question.

In Part D of this paper, we return to the details of the notice and consent framework as implemented in the APPs, and how that framework could be changed to improve data privacy outcomes for individuals.

PART C– THE INTERACTION OF CHOICE, RIGHTS AND SOCIETAL INTERESTS

4 Factoring rights into our discussion

In section 3.7 above, we observed that data privacy regulation should protect both individual interests and social or collective interests. We noted Professor Helen Nissenbaum's argument that privacy is a set of social norms, not a set of individual decisions.

It is no means self-evident *how* data privacy regulation should protect both individual interests and social or collective interests and also take into account the societal interest in a vibrant digital economy.

This Part C discusses how an individual 's right not to be subject to privacy harms could be better tied to the Australian Privacy Principles.

4.1 Individual rights, societal interests and a vibrant digital economy

A good starting point to discussion of privacy rights and harms is the discussion of the Committee of Experts of India tasked with development of the Data Protection Bill 2019 of India. The Committee expressed the importance of understanding the societal basis of data privacy rights of individuals, and balancing that societal interest against the interests of society in a vibrant digital economy, as follows:

> It is our view that any [data privacy regulatory] regime that is serious about safeguarding personal data of the individual must aspire to the common public good of both a free and fair digital economy.
>
> Fairness pertains to developing a regulatory framework where the rights of the individual with respect to her personal data are respected and the existing inequality in bargaining power between individuals and entities that process such personal data is mitigated. In such a framework, the individual must be the "data principal" since she is the focal actor in the digital economy. The relationship between the individual and entities with whom the individual shares her personal data is one that is based on a fundamental expectation of trust.
>
> Notwithstanding any contractual relationship, an individual expects that her personal data will be used fairly, in a manner that fulfils her interest and is reasonably foreseeable. This is the hallmark of a fiduciary relationship. In the digital economy, depending on the nature of data that is shared, the purpose of such sharing and the entities with which sharing happens, data principals expect varying levels of trust and loyalty. For entities, this translates to a duty of care to deal with such data fairly and responsibly for purposes reasonably expected by the principals. This makes such entities "data fiduciaries".

> Pursuant to this, and as a general canon, data fiduciaries must only be allowed to share and use personal data to fulfil the expectations of the data principal in a manner that furthers the common public good of a free and fair digital economy. It is our considered view that a regime based on the principles mentioned above and implemented through the relations described above will ensure individual autonomy and make available the benefits of data flows to the economy…. .
>
> The twin objectives of protecting personal data while unlocking the data economy have often been seen as conflicting with each other… .
>
> In our view, ensuring the protection of personal data and facilitating the growth of the digital economy are not in conflict and has rightly been pointed out, serve a common constitutional objective. However, each of them is motivated by distinct intermediate rationales — the former ensuring the protection of individual autonomy and consequent harm prevention and the latter seeking to create real choices for citizens. Both these intermediate objectives themselves are complementary — individual autonomy becomes truly meaningful when real choice (and not simply an illusory notion of it) can be exercised and likewise no real choice is possible if individuals remain vulnerable. The growth of the digital economy, which is proceeding apace worldwide, must be equitable, rights-reinforcing and empowering for the citizenry as a whole. In this, to see the individual as an atomised unit, standing apart from the collective, neither flows from our constitutional framework nor accurately grasps the true nature of rights litigation.[47]

This reasoning reflects Indian jurisprudence following the landmark Supreme Court of India judgement in Justice K.S. Puttaswamy (Retd.) v. Union of India,[48] which recognised a fundamental right to privacy implicit within Article 21 of the Constitution of India.[49]

4.2 Is privacy as a fundamental right relevant to applying the APPs?

The Australian Constitution has no counterpart provision to Article 21 addressing personal liberty or personal dignity.

The Australian Parliament has not enacted a right of Australian citizens in and to data privacy, or to be protected from privacy harms, as statutory entitlements.

[47] A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians, Report of Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, pages 7-9

[48] 2017 (10) SCALE 1

[49] Article 21 of the Constitution of India, 1950 provides that "No person shall be deprived of his life or personal liberty except according to procedure established by law". This article has been compared to the Magna Carta of 1215, the Fifth Amendment to the American Constitution, Article 40(4) of the Constitution of Eire 1937, and Article XXXI of the Constitution of Japan 1946

The Australian Parliament has not enacted a baseline human rights statute against which all data privacy impacting acts and practices must be considered.

Contrast the position in the European Union, where jurisprudence of the European Court of Justice effectively gives primacy of Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union, which provide that everyone has the right to the protection of personal data concerning him or her. The GDPR cannot be read or applied without understanding that this 'fundamental right' prevails over all the permitted grounds for data processing as expressly stated in the GDPR, including consent and legitimate interests.

Accordingly, provisions of the GDPR are a useful reference point in regulatory design of data privacy provisions in Australia, but provisions of the GDPR cannot simply be 'copied over' to have analogous effect and operation under Australian law.

Of course, data privacy is protected under various international instruments, including the United Nations Declaration of Human Rights 1948 and the United Nations International Convention on Civil and Political Rights 1966 (**ICCPR**). Australia is a signatory to both instruments.

Article 17 of the ICCPR provides:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

The Recitals to the Privacy Act 1988 note that Australia, by becoming a party to the ICCPR, undertook to adopt such legislative measures as may be necessary to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence.

Section 2A of the Privacy Act 1988 sets out the objects of the Act, which include:

> (a) to promote the protection of the privacy of individuals; and
>
> (b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities; and
>
> (c) to provide the basis for nationally consistent regulation of privacy and the handling of personal information; and
>
> (d) to promote responsible and transparent handling of personal information by entities;

……..

(h) to implement Australia's international obligation in relation to privacy.

This statement of objects not explicitly tied to the operative provisions of the Privacy Act 1988.[50] Absence of an express tie is a problem.

Contrast some analogous statutes.

The Personal Information Protection and Electronic Documents Act of Canada (**PIPEA**) relevantly provides:

PART 1 Protection of Personal Information in the Private Sector

…..

Purpose

3 The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure 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

….

Appropriate purposes

5(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.[51]

….

Valid consent

6.1 For the purposes of clause 4.3 [PIPEDA Fair Information Principle 3 – Consent"] of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the

[50] Indeed, the Act as enacted does not include this statement of objects: section 2A was included in the Act only in 2012, so the link between the data protection principles as stated in the Act, and the more abstract concept of privacy, was even more tenuous before 2012 than it is today

[51] See further OPC, Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), May 2018, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/

nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

In applying subsection 5(3), Canadian courts have generally taken into consideration whether the collection, use or disclosure of personal information is directed to a bona fide business interest, and whether the loss of privacy is proportional to any benefit gained.[52] The following factors have been stated to determination of whether an organization's purpose complies with subsection 5(3):

- the degree of sensitivity of the personal information at issue;
- whether the organization's purpose represents a legitimate need / bona fide business interest;
- whether the collection, use and disclosure would be effective in meeting the organization's need;
- whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits; and
- whether the loss of privacy is proportional to the benefits.[53]

The Office of the Privacy Commissioner (**OPC**) of Canada has stated an interpretation of subsection 5(3) that includes certain so-called 'no-go zones', including:

- "that a reasonable person would not consider it appropriate for organizations to require an individual to undergo significant privacy harm as a known or probable cost for products or services. By "significant harm", we mean "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on (one's) credit record and damage to or loss of property".[54] "If an organization identifies potential harms that may arise from the collection, use or disclosure of personal information, PIPEDA's accountability principle[55] will require that the organization will seek to minimize this risk. In some cases, mitigation efforts will reduce the risk significantly. In other cases, the risk will remain meaningful. Only meaningful residual risks of significant harm must be

[52] Ibid, under heading "Evaluating an organization's purposes under 5(3)"; A.T. v. Globe24h.com, 2017 FC 114
[53] A.T. v. Globe24h.com, 2017 FC 114 at [74]; Ibid; also Turner v. Telus Communications Inc., 2005 FC 1601, ¶39, aff'd 2007 FCA 21, at [48]
[54] OPC, Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), May 2018, under heading "3. Collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual"
[55] OPC, PIPEDA Fair Information Principle 1 – Accountability, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/

notified to individuals. By meaningful risk, we mean a risk that falls below the balance of probabilities but is more than a minimal or mere possibility."[56]

- that "w]hile profiling that leads to discrimination contrary to human rights law will always be inappropriate under 5(3), determining whether a result is unfair or unethical will require a case-by-case assessment. Organizations should know, however, that unfair or unethical profiling or categorization will also generally be found inappropriate under subsection 5(3),[57]
- surveillance by an organization through audio or video functionality of the individual's own device. "Nothing can be more privacy-invasive than being tracked through the audio or video functionality of an individual's device either covertly, that is without their knowledge or consent, or even with *so-called* consent, when doing so is grossly disproportionate to the business objective sought to be achieved. … It may be permissible for the audio or video functionality of a device to regularly or constantly be turned on in order to provide a service if the individual is both fully aware and in control of this fact, and the captured information is not recorded, used, disclosed or retained except for the specific purpose of providing the service.[58]

In applying subsection 6.1, the OPC has stated that the appropriate form of consent is express (explicit) consent for collections, uses or disclosures which:

- involves sensitive information;
- are outside the reasonable expectations of the individual; and/or
- create a meaningful residual risk of significant harm.[59]

These (currently operative) Canadian statutory provisions significantly extend data privacy protections for Canadian beyond the notice and consent framework as implemented in the Australian Privacy Principles.

However, and notwithstanding these current further protections, the Office of the Privacy Commissioner of Canada in the Office's 2018-2019 Annual Report to Parliament proposed further reform of PIPEA to be "rights-based legislation with the following key elements":

> Define the right to privacy in its broadest sense, which means to make explicit that a central purpose of the law should be to protect privacy as a human right in and of

[56] OPC, Guidelines for obtaining meaningful consent, sub-heading "Risk of harm and other consequences" under "1. Emphasize key elements", https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805

[57] Ibid, under heading "2. Profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law"

[58] Ibid, under heading "6. Surveillance by an organization through audio or video functionality of the individual's own device"

[59] OPC, Guidelines for obtaining meaningful consent, heading "Determining the appropriate form of consent", also citing Royal Bank of Canada v. Trang, 2016 SCC 50 § 23

itself, and as essential for the realization and protection of other human rights. A broad definition of privacy, consistent with the Finestone Charter[60], could include "freedom from surveillance, without justification", these last two words confirming that privacy is not an absolute right. Finally, a definition of privacy as a right would be reflective of the rich jurisprudence on this subject, including by the Supreme Court of Canada.

Recognize in law the quasi-constitutional nature of privacy legislation, which means confirming the protected status of privacy as established through decisions of the Supreme Court of Canada, where the Court recognized the fundamental role privacy plays in the preservation of a free and democratic society.

Draft the law in the usual manner of legislation, conferring rights and imposing obligations, rather than as the current model, which contains what reads as an industry code of conduct, with some obligations but also several recommendations, examples and good practices that do not create enforceable entitlements for individuals. Courts have also noted that, due to its non-legal drafting, PIPEDA is not an easily accessible statute and gives little, if any guidance at all, to those who must interpret it.

Ensure effective enforcement, which means adopting enforcement mechanisms that would result in quick and effective remedies for individuals, and broad and ongoing compliance for organizations and institutions. Without effective enforcement, rights become hollow and trust dissipates.[61]

[60] A proposal for a Canadian Charter of Privacy Rights, promoted by Senator Sheila Finestone in the late 1990s as Bill S-21 of the Senate of Canada, 2001 (https://www.parl.ca/DocumentViewer/en/37-1/bill/S-21/first-reading/page-24). The Bill proposed a Right to privacy, expressed in clause 3 as "Every individual has a right to privacy, including (a) physical privacy; (b) freedom from surveillance; (c) freedom from monitoring or interception of their private communications; and (d) freedom from the collection, use and disclosure of their personal information. Infringement. Clause 5 provided that "A limit on or interference with an individual's privacy infringes that individual's right to privacy, but "(2) An infringement of an individual's right to privacy is justifiable if the infringement is reasonable and can be demonstrably justified in a free and democratic society. Clause 5(3) provided that "(3) An infringement is justifiable if (a) it is lawful; (b) it is necessary to achieve an objective that is compelled by the need to respect another individual human right or another interest in the public good and is sufficiently important to warrant infringing the right to privacy; (c) the objective cannot be achieved by another measure that infringes privacy less; and (d) the importance of the objective and the beneficial effects of the infringement outweigh the detrimental effects on privacy". Clause 5(4) provided that "(4) An interference with an individual's privacy does not infringe that individual's right to privacy if the interference is done with the free and fully informed consent of the individual." The Bill lapsed when the 37th Parliament was prorogued.

[61] Office of the Privacy Commissioner of Canada, Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy, 2018-2019 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act, available at https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/

The OPC, in a January 2020 call for submissions, sought views as to when "the current consent model may not be viable in all situations, including for certain uses of AI", and accordingly alternative grounds, such as GDPR's legitimate interests[62], might be appropriate. The OPC stated:

> We believe there is a continued role for consent in the use of AI when it can be meaningful, and, to that extent, we would support efforts by the federal government to explore incentivizing new business models that promote innovative consent models. For example, emerging consent technologies and personal information management systems offer important opportunities to preserve human agency and meaningfully inform individuals about the development and deployment of AI systems. These approaches should be maximized to facilitate consent whenever possible.
>
> That said, and as outlined in our Report on Consent[63], we acknowledge that alternate grounds to consent may be acceptable in certain circumstances, specifically when obtaining meaningful consent is not practicable and certain preconditions are met. In our Report we proposed that Parliament consider amending PIPEDA to introduce new exceptions to consent to allow for socially beneficial activities that the original PIPEDA drafters did not envisage. Such alternative grounds would not be intended to relax privacy rules but rather to recognize that consent may not be effective in all circumstances and that more effective measures must be adopted to better protect privacy.
>
> In assessing how a future PIPEDA should appropriately deal with consent, particularly in the AI context, we propose that meaningful consent should be required in the first instance for transparency and to preserve human agency. Alternative grounds for processing such as those found in the GDPR and outlined in our Report on Consent should be available in instances where obtaining meaningful consent is not possible and prescribed conditions, such as demonstrating that obtaining consent was

[62] Article 6(1)(f) of the GDPR states: "1.Processing shall be lawful only if and to the extent that at least one of the following applies: …(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." ICO UK suggest that this is a three part test to be applied in the following order: "Purpose test – is there a legitimate interest behind the processing? Necessity test – is the processing necessary for that purpose? Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms? See further ICO UK, What is the 'legitimate interests' basis? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

[63] Office of the Privacy Commissioner of Canada, 2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act under heading "Report on Consent", https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/

considered and impracticable and that a PIA was conducted and published in advance, are first met".

The use of non-identifiable data, such as through the application of de-identification methods, could also be a factor in determining whether certain other grounds for processing such as legitimate or public interest should be authorized under the Act.

A new consent exception of this nature would necessarily have to be contingent on stronger enforcement powers that would authorize the privacy regulator, where warranted, to assess whether the use of personal information was indeed for broader societal purposes and met the prescribed legal conditions.[64]

A more modest attempt to give effect to data privacy as a right within a broadly similar data privacy statute to the Privacy Act 1988 can be seen in the proposed provisions of the Privacy Bill of New Zealand as currently before the NZ Parliament.

The relevant provisions state:

3 Purpose of this Act

The purpose of this Act is to promote and protect individual privacy by—

(a) providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognising that other rights and interests may at times also need to be taken into account; and

(b) giving effect to internationally recognised privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines and the International Covenant on Civil and Political Rights.

…….

Information privacy principle 4 - Manner of collection of personal information

(1) An agency may collect personal information only—

(a) by a lawful means; and

(b) by a means that, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons),—

[64] OPC, "Consultation on the OPC's Proposals for ensuring appropriate regulation of artificial intelligence: Seeking views on the OPC's recommendations to Government/Parliament" under heading "Proposal 7: Include in the law alternative grounds for processing and solutions to protect privacy when obtaining meaningful consent is not practicable", https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_ai_202001/

(i) is fair; and

(ii) does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Proposed IPP 4 has drafting limitations. In particular, the draft provision replicates the problem with APP 3.5 (An APP entity must collect personal information *only by lawful and fair means*) by focusing only upon the *means* of collection, and not the *outcome* (the end) effected through a subsequent use or disclosure and which is where adverse data privacy impacts are experienced. PIPEA section 5(3) (An organization may *collect, use or disclose* personal information only for purposes that a reasonable person would consider are appropriate in the circumstances) is a better provision in that the provision also addresses uses and disclosures.

4.3 RECOMMENDATION 1: Bringing privacy rights and harms explicitly into the APPs

A composite provision to supplement the APPs might be:

> An APP entity may engage in an act or practice of collection, use or disclosure of personal information about individuals, including an act or practice of differentiation as between individuals using data or algorithmic methods derived from analysis of personal information about individuals[65], only to the extent:
>
> (a) that personal information is collected by a means that is fair and lawful; and
>
> (b) where in the circumstances of the case (and particularly in circumstances where that personal information is about affected persons that are young, vulnerable or at risk):
>
> (i) the affected individual will not suffer significant harm as a known or reasonably likely outcome from collection, use or disclosure of that personal information, whether that significant harm arises directly through an act or practice of that APP entity or indirectly through an act or practice of another entity reasonable attributable to collection, use or disclosure of that personal information by the APP entity;
>
> (ii) the collection, use or disclosure does not intrude to an unreasonable extent upon the personal affairs of the affected individual; and

[65] This inclusion is intended to capture individuation enabled through pseudonymisation and personalisation through use of algorithms derived from training data, in circumstances where this use may occasion what Marty Abrams refers to as 'consequential harm'. See Marty Abrams, Privacy Law Must Focus Upon Consequential Harm, Information Accountability Foundation blog post of 2 June 2020.

(iii) a reasonable person would consider the collection, use or disclosure appropriate in the circumstances.

(c) In applying paragraph (b) to an act or practice of collection, use or disclosure of personal information about an individual, including acts or practices an APP entity should have regard to each of the following:[66]

(i) the likelihood of a privacy harm arising from that act or practice and the extent of its impact upon an affected individual;

(ii) whether any significant effect upon an affected individual is reasonably likely to be likely to be understood by an affected individual;

(iii) whether the act or practice is transparent to an affected individual;

(iv) whether the affected individual has provided unambiguous affirmative consent to the particular acts or practice;

(v) whether the act or practice is beneficial to an affected individual;

(vi) whether the act or practice provides societal benefits or creates or contributes to societal detriments (such as erosion of trust of citizens in use of online services);[67]

(vii) whether the act or practice is consistent with the context of the relationship between the individual and the APP entity;

(viii) whether the act or practice is in fulfilment of a legitimate business purpose and the effect of the act or practice is necessary and proportionate to fulfilment of that legitimate business purpose;

[66] The selection of factors listed in this provision has been influenced by the excellent work of the Information Accountability Foundation and in particular the IAF's Sept. 23, 2019 draft 'Fair Accountable Innovative Responsible and Open Processing Enabling New Uses that are Secure and Ethical 16 Act' or 'FAIR and OPEN USE Act'. The author acknowledges his debt to Marty Abrams and the IAF team.

[67] The IAF Fair and Open Use Act suggests a definition of the term "societal benefit" as "a material, objective, and identifiable positive effect or advantageous outcome accruing to the public as a result of the processing of personal data. To meet the requirements of this Act, a societal benefit must: (A) promote and enhance the well being of the general public; and (B) be separate and distinct from any positive outcome, advantageous impact, or value that accrues to a covered entity, single person or individual, or a narrow or specific group of persons. (2) Examples of factors that may be considered include greater access to health care; better or lower cost health care; improvements to the general welfare; improvements to education; environmental enhancements, such as water conservation; energy cost reduction; protection of rights; and improved services or ease of use of services: page 13, lines 354-367 of 23 September 2019 draft.

(ix) whether the APP entity has established, implemented, tested, revised, and documented reasonable and appropriate policies, procedures, and technical controls and safeguards, taking into account the purpose of the act or practice and the level of risk;

(x) the effect of technical, operational, legal and other controls and safeguards, taken as a whole, to mitigate risk of privacy harms arising from the act or practice and to manage residual risks which cannot reasonably be mitigated;

(xi) any guidance published by the Commissioner in relation to this provision.

The key concepts of *a right of data privacy* and *privacy harms* are explored in the paper accompanying this paper.

PART D – IMPROVING NOTICE AND CONSENT

5 Notice and consent around the globe

Most data privacy statutes enacted around the globe over the last four decades are based a notice and consent framework.

The notice and consent framework as enacted in data privacy statutes around the globe has many variants that have evolved over time in response to increasingly cross border provision of services (challenging jurisdictional differences between jurisdictions as to particular requirements) and changes in:

- range and capacity in data handling and in data applications,
- new collections of data and uses of data, and in particular expansion of multi-party, product or service supply side data ecosystems,
- growth of secondary uses and markets for secondary uses of consumer data,
- levels of trust of consumers and citizens with organisations with whom they interact or deal, and with organisations that provide platforms over which consumers and citizens interact with each other, and in particular challenges to digital trust as to fair, socially responsible, and transparent uses of data about individuals, including fair sharing of economic and business benefits as between data collector or user and the affected individual,
- access technologies, and in particular the explosive growth in capabilities and uses of small screen devices such as smartphones, with the twin effects of making notices to consumers less likely to be read and enabling ever more privacy affecting uses and sharing of data about individuals and affecting how they are treated, including but not only personal information about identifiable individuals,[68]
- the extent of perceived or actual dependence of consumers upon certain online services, and in particular social media platforms, search engines, cloud consumer services such as streamed entertainment services and cloud storage services, online commerce, and more recently personal wellness services, home smart speakers and other digital assistant and IoT services,
- rapid expansion and take up of IoT services where the individual or household that is observed or monitored may not be the controller or enabler of the relevant device, may not even be aware that the individual is being observed or monitored, or how insights or

[68] See further Leonard, Peter, "Jobs Half Done: Getting Smart about Smartphones", Computers and Law (UK Society for Computers and the Law), December 2019; Leonard, Peter, "Data Ownership and the Regulation of Data Driven Businesses", Scitech Lawyer (American Bar Association), 16/2, Winter 2020

other inferences about that household's or individual's behaviour may be used to affect how they are treated relative to others,

- expectations of some consumers and civil society organisations as to consumer control and choice.

The notice and consent framework applies free market defaults of 'freedom of contract' and 'consumer choice' and:

- empowers individuals to know when, why and how personal information about them is being collected and handled,
- creates an incentive for business restraint, and facilitates regulatory oversight, as published privacy statements and policies create transparency as to when, why and how personal information about citizens is being collected and handled,
- reduces the information burden upon individuals, by dispensing with requirements as to notice or consent in limited exempt circumstances (as specified by the data privacy statute or expressly contemplated by another law),
- limits the legal requirement to obtain consent to fewer, higher risk or impact circumstances, such as handling of sensitive personal information, and
- reduces barriers to global commerce, and barriers to cooperation and coordination across-borders in regulatory action and enforcement, by ensuring that there are common policy underpinnings and elements in privacy rules, even though well short of a universal approach.

Older data privacy statutes, including the Privacy Act 1988 (C'th of Australia), the Privacy Act 1993 (NZ), the Personal Data (Privacy) Ordinance (Cap. 486) (Hong Kong SAR China), and the Personal Information Protection and Electronic Documents Act 2000 (Canada), reflect the notice and consent framework as derived from the North American concept of Fair Information Practices[69] and expanded in the Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (as adopted in 1980).[70] Those statements sought to effect a policy balance

[69] Summarised at https://iapp.org/resources/article/fair-information-practices/. See Federal Trade Commission, Privacy Online: A Report to Congress, June 1998, available at https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf; also Cate, Fred H., The Failure of Fair Information Practice Principles, Chapter 13 from Consumer Protection in the Age of the Information Economy (2006), available at https://www.ftc.gov/system/files/documents/public_comments/2018/12/ftc-2018-0098-d-0036-163372.pdf; also Gellman, Robert, Fair Information Practices: A Basic History, Version 2.19, October 7, 2019, https://bobgellman.com/rg-docs/rg-FIPshistory.pdf

[70] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980 at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpers

between the 'fundamental but competing values' of 'privacy and the free flow of information'. That policy balance is generally effected in data privacy statutes implementing the notice and consent framework through enactment of legal rules:

- as to circumstances in which handling of personal information about an individual is explicitly permissible without any notice, without notice but without consent, or only with consent,
- as to circumstances in which an individual is to be taken to give consent to other handling of personal information about that individual. These circumstances typically require the regulated entity to inform the affected individual of the reason, context and purpose of the proposed handling of personal information, and specify requirements as to the form and contents of a request for consent and the form and other characteristics of a valid consent as provided by the individual.

Typically, the legal rules as to when handling of personal information about an individual is explicitly permissible do not require notice to be given to an individual as to some forms of handling of personal information – for example:

- general permitted situations (section 16A) and permitted health situations (section 16B) specified in the Privacy Act 1988,
- as specifically required or authorised by another law,
- for secondary purposes directly related to a primary permitted (through notice or consent, as required) purpose.

The effect of the legal rules is to create a (qualified) right of an affected individual:

- to know when and how particular types of personal information about the individual are collected and handled by a regulated entity,
- to consent, or not consent, to a specified sub-set of those particular types of personal information being collected and handled by a regulated entity.

Some statutes, recognising the fundamental right to privacy, seek to ensure that the legislature does not inadvertently override operation of the statutory protections. The Personal Information Protection and Electronic Documents Act of Canada provides:

> 4(3) Every provision of this Part applies despite any provision, enacted after this subsection comes into force, of any other Act of Parliament, unless the other Act expressly declares that that provision operates despite the provision.

onaldata.htm; as revised in 2013 at http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm, see also Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data No. 108, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 and as 'modernised' in 2018 at https://www.coe.int/en/web/data-protection/convention108/modernised

Many of the notice and consent framework statutes, including the Privacy Act 1988, effect the notice and consent framework through statement of 'principles' that in practice operate as broadly stated legislated rules.

A typical feature of those statutes is to:

- describe circumstances in which regulated entities that collect, use and otherwise handle or disclose ('handle' or 'process') personal information about individuals must give notice to those individuals as to that handling of personal information, with varying approaches to what matters must be addressed in a notice at collection and what matters must be addressed in a privacy policy, and
- in a sub-set of those circumstances, require the regulated entity to obtain consent of the affected individual (data subject), with varying approaches to requiring granularity of consent (consent separated from acceptance of other, less privacy affecting, terms) and to whether there must be an affirmative demonstration of consent of the affected individual.[71]

Another typical feature of those statutes is to specify this sub-set of those circumstances (where consent is required) as being:

- where there is to be a collection and handling (processing) of statutorily specified categories of personal information, often being categories of personal information where collection and handling are regarded as of higher sensitivity to, or of greater impact upon, the data subject;
- where personal information is collected from a third party – that is, other than from the affected individual.

Areas of variance in regulatory design as to notices at collection include:

- The relationship of a regulated entity's general privacy policy and notices at collection – in particular, the extent to which relevant information can be omitted from a notice at collection because it is already addressed in a regulated entity's privacy policy, which items must be addressed in both, how the two may cross-reference each other, and the extent to which a change in one must be reflected in the other.
- The specified categories of handling of personal information in relation to which regulated entities must give notice at collection to affected individuals.
- The ways in which notice is required to be given or may be given, and specifically, any division and allocation of covered matters between a general notice as to a regulated entity's policies and processes for handling of personal information, any notice as to

[71] For example, Japan, Act on the Protection of Personal Information, Article 17 (2), "A personal information handling business operator shall, except in those cases set forth in the following, not acquire special care-required personal information without obtaining in advance a principal's consent".

policies and processes for handling of personal information particular to a provision of a particular product or service, and any notification specific to an interaction between a regulated entity and an individual.

- The style and form of the notice (multi-layered etc.).
- The level of detail required in the notice.
- The timeliness of the notice i.e. posted generally, or available if an individual makes an election to look, or posted adjacent to a particular provision or interaction, affirmatively provided (pushed) or otherwise provided 'just-in-time'.
- Whether a new notice should be pushed to an individual in relation to a change in handling practices.
- Whether new notice must only be pushed in relation to personal information subsequently collected or also in relation to new handling of existing holdings of personal information.
- The extent of notice required to be given by the collecting entity as to the nature and range of possible downstream uses of personal information by entities to whom the collecting entity may elect to disclose personal information, or whether the notice by the collecting entity need only be of that prospective disclosure (with uses and disclosures by the downstream entity then addressed in a separate notice given by the downstream entity).
- Whether notice is required of other circumstances in which personal information may be used in manners potentially adverse to the interests or expectations of the individual – for example, of uses of deidentified information to effect specific (individualised) outcomes adverse to an affected individual or small cohorts of like individuals as compared to other groups of individuals, such as denial of supply of a particular product or service, or less advantageous prices or other terms for a particular product or service.
- Whether notice is required as to the nature and extent of disclosures of personal information as may be legally required to be made by the collecting entity and which might reasonably affect a decision made by the collecting entity.
- The circumstances in which an individual should be provided a choice as to whether to provide personal information or authorise or permit personal information to be used (although data privacy statutes almost invariably include a variant of the data minimisation).

Areas of variance in regulatory design as to as to consent include:

- The specified categories of handling of personal information for which consent of affected individuals must be obtained.

- Whether consent must be given explicitly; if so, whether in writing or orally; and how it may be evidenced. Generally, a regulated entity carries the evidentiary burden of proving that consent where required was obtained.
- Whether and to what extent consent must be unbundled from provision of a service to be considered to be voluntarily given.
- Whether and to what extent to which consent as to individual categories of uses or other handling of personal information must be unbundled from consent to other categories of uses or other handling to be considered to be voluntarily given.
- the extent to which consent is permitted to be inferred, the circumstances in which it may be inferred, and in particular the adjacency and timeliness of the statement of prospective uses to the act of the individual from which an affirmative response permitting those prospective uses is inferred.
- Whether pre-ticked consent boxes are allowed, or the default should always be to no consent.
- Each of the variants listed above in relation to notices, but specific to circumstances in which consent is required.
- Whether there are statutory no-go zones, such as particular collection and handling of some specified categories of personal information, in relation to which consent cannot be sought or will not be effective.
- Whether there is a further sub-division in the class of categories of personal information requiring consent to which a higher threshold of consent apply.

6 Refocussing notice and consent

6.1 Flexibility in categories of personal information that are sensitive information

More recent data privacy statutes and legislative proposals demonstrate a trend away from a stated, exhaustive, list of categories of personal information that are deemed to be sensitive information[72] in relation to which consent must be obtained, towards either:

- stating criteria for an assessment by a regulated entity as to whether particular acts or practices carry higher risks or impacts[73] and therefore should be:
    - ♦ the subject of specific consent, or

[72] E.g. Definition of ''sensitive information" in section 5 of the Privacy Act 1988 and special categories of data in Articles 8 and 9 of the GDPR. See also the requirement to perform a Data Protection Impact Assessment in relation to large scale processing of special categories of data: Article 35(3)(b) of the GDPR.

[73] Assessment of data privacy risks, impacts and harms is addressed in the related paper to this paper

- the subject of an impact assessment[74] and then the subject of specific consent if any residual risk (after mitigation in accordance with the findings of that assessment) is greater than a particular higher threshold as specified by the statute,

- stating a list of categories of sensitive information which is not closed and empowering either the legislature or regulator to add to the list by making a subordinate instrument (a regulation, directive or other formal instrument).[75]

Relevant policy considerations are summarised by the Committee of Experts of India as follows:

> While there has been no clear-cut approach towards categorising sensitive personal data, some authors have suggested a contextual approach, i.e., where any personal data can become sensitive depending on the circumstances and the manner in which it is being processed.
>
> However, this approach may place significant burden on data fiduciaries and regulatory resources as they would have to determine whether the personal data in question is sensitive or not, and whether it is capable of causing great harm to the individual, on a case by case basis. Therefore, by identifying certain types of data as sensitive in the law itself, and setting out specific obligations that must be met by the

[74] For example, GDPR ; Personal Data Protection Bill 2019 of India (as introduced into the Lok Sabha), section 27(1), "Where the significant data fiduciary intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data principals, such processing shall not be commenced unless the data fiduciary has undertaken a data protection impact assessment in accordance with the provisions of this section".

[75] See for example Japan, Act on the Protection of Personal Information, Article 2(3), "'Special care-required personal information' in this Act means personal information comprising a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, *or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal*", Korea (South), Article 23, "The personal information controller shall not process the personal information (hereinafter referred to as the "sensitive data") including ideology, belief, admission/exit to and from trade unions or political parties, political mindset, health, sexual life, and other personal information which is likely doing harm to privacy of data subjects as prescribed by the Presidential Decree….."; Personal Data Protection Bill 2019 of India (as introduced into the Lok Sabha), section 1(36) "'sensitive personal data' means such personal data, which may, reveal, be related to, or constitute - (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under section 15."; Pakistan, Personal Data Protection Bill 2020, Consultation Draft v.09.04.20, "''sensitive personal data' means and includes data relating to access control (username and/or password), financial information such as bank account, credit card, debit card, or other payment instruments, and, passports, biometric data, and physical, psychological, and mental health conditions, medical records, and any detail pertaining to an individual's ethnicity, religious beliefs, or any other information [specified by regulation] for the purposes of this Act and rules made thereunder."

data fiduciary while processing such data, potentially significant harms may be pre-empted.

Data sensitivity, in one view, can depend on the legal and sociological context of a country. However, certain categories of personal data are capable of giving rise to privacy harms regardless of context and an objective method of identifying such kinds of data becomes necessary. Hence, we have considered the following criteria to categorise what is 'sensitive':

(i) the likelihood that processing of a category of personal data would cause significant harm to the data principal;

(ii) any expectation of confidentiality that might be applicable to that category of personal data;

(iii) whether a significantly discernible class of data principals could suffer harm of a similar or relatable nature;

(iv) the adequacy of general rules to personal data.[76]

The Committee listed certain categories of personal data[77] and recommended inclusion of a provision which now appears as clause 15 (Categorisation of personal data as sensitive personal data) of the Personal Data Protection Bill 2019 of India, as introduced into the Lok Sabha, states:

15. (1) The Central Government shall, in consultation with the Authority and the sectoral regulator concerned, notify such categories of personal data as "sensitive personal data", having regard to—

(a) the risk of significant harm that may be caused to the data principal by the processing of such category of personal data;

(b) the expectation of confidentiality attached to such category of personal data;

(c) whether a significantly discernible class of data principals may suffer significant harm from the processing of such category of personal data; and

(d) the adequacy of protection afforded by ordinary provisions applicable to personal data.

[76] A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians, Report of Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, pages 30-31; also citing Paul Ohm, "Sensitive Information", 88 Southern California Law Review (2015)
[77] See preceding footnote.

> (2) The Authority may specify, by regulations, the additional safeguards or restrictions for the purposes of repeated, continuous or systematic collection of sensitive personal data for profiling of such personal data.

This provision reflects the following explanation by the Committee of Experts:

> "[This] residuary power will be vested with the DPA to list out further categories of sensitive personal data on the basis of the above criteria. This power has been considered necessary due to the impracticability of laying down an exhaustive enumeration at the time of drafting. Harm can be caused by the processing of sensitive personal data per se or if it is aggregated for profiling. Consequently, the DPA will be granted a residuary power to list categories of sensitive personal data on the basis of both these sources of harm, as and when it considers necessary. Thus, for instance, geo-location data may be considered for listing as a category of sensitive personal data in the future since it may lead to harm upon aggregation.[78]

6.2 Flexibility as to matters to be addressed in privacy notices and privacy policies

Given the range of circumstances in which APP 5 notices are required to be given, it may be questioned whether the APP setting of prescriptively providing, with economy wide effect, the categories in information to be addressed in an APP 5 notice is in the best interests of customers.

Less information, better targeted to address key concerns, with regulated entities conferred broader discretion (with concomitant responsibility and legal accountability of regulated entities) to determine what is key or essential information, may better address concerns and interests of affected individuals, and increase the likelihood that APP 5 notices will be read and comprehended by affected individuals.

If there is concern that this approach might leave too much discretion or provide insufficient guidance to regulated entities as to APP 5 notices, an alternative approach might be to afford regulated entities an option, namely for each required APP 5 notice, a right to elect either to:

- to include all categories of information as prescribed for an APP 5 notice, or
- to include only such essential or key terms as ought reasonably be drawn to the attention of reasonably anticipated affected individuals.

A further legislative innovation might be to empower the OAIC to change the list of categories of information as prescribed for inclusion in an APP 5 notice, either generally

[78] A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians, Report of Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, page 32.

(economy wide) or in relation to particular products, services or other acts or practices as may be determined by the OAIC.

A similar legislative innovation might also be considered in relation to the list of matters in APP 1.4 for mandatory inclusion in a privacy policy.

Any such regulatory change to empower the OAIC to change the list of categories of information as prescribed for inclusion in an APP 5 notice, and to change the list of matters in APP 1.4 for mandatory inclusion in a privacy policy, should allow both for addition or removal of particular categories of information, both generally (economy wide) or in relation to particular products, services or other acts or practices as may be determined by the OAIC. A precondition to exercise of that discretion should be prior public consultation.

The Privacy Bill No. 373 of 2019 of New Zealand provides a useful analogy, albeit that this analogy is focussed upon codes of practice:

> 35 Codes of practice in relation to IPPs
>
> (1) The Commissioner may at any time issue a code of practice in relation to the IPPs.
>
> (2) A code of practice may—
>
> (a) modify the application of 1 or more of the IPPs by:
>
> (i) prescribing more stringent or less stringent standards:
>
> (ii) exempting any action from an IPP, either unconditionally or conditionally:
>
> (b) apply 1 or more of the IPPs without modification;
>
> (c) prescribe how 1 or more of the IPPs are to be applied or complied with.
>
> (3) A code of practice may apply in relation to 1 or more of the following:
>
> (a) any specified information or class or classes of information;
>
> (b) any specified agency or class or classes of agency;
>
> (c) any specified activity or class or classes of activity;
>
> (d) any specified industry, profession, or calling or class or classes of industry, profession, or calling.
>
> 38 Issue of code of practice
>
> (1) The Commissioner may issue a code of practice under section 35 or 36 on—
>
> (a) the Commissioner's own initiative; or
>
> (b) the application of any person.

(2) An application may be made under subsection (1)(b) only—

(a) by a body that represents the interests of any class or classes of agency, industry, profession, or calling (a group); and

(b) if the code of practice sought by the applicant is intended to apply to that group, or any activity of the group.

(3) Before issuing a code of practice, the Commissioner must—

(a) give public notice of the Commissioner's intention to issue the code and include a statement that—

(i) the details of the proposed code, including a draft of the proposed code, may be obtained from the Commissioner; and

(ii) submissions on the proposed code may be made in writing to the Commissioner within the period specified in the notice; and

(b) do everything reasonably possible to advise all persons affected by the proposed code, or the representatives of those persons, of—

(i) the details of the proposed code; and

(ii) the reasons for the proposed code; and

(c) give the persons affected by the code, or the representatives of those persons, the opportunity to make submissions on the proposed code; and

(d) consider any submissions made on the proposed code.

Advocacy for a more individual-focussed and distinct role for a notice at collection, and a more regulatory focussed role for a privacy policy, should not be taken as this paper endorsing obtusely legalistic and lengthy privacy policies. The distinction as to the functions, and therefore contents, of privacy policies and notices at collection does not mean that a privacy policy should be allowed to become (or remain) an impenetrable regulatory statement, or that a privacy notice should be drafted as though an individual should never be expected to read a privacy policy.

The American Law Institute's "Tentative Draft" Principles of Law, Data Privacy[79] propose a nuanced approach to privacy disclosures, differentiating between a 'transparency

[79] The full Principles (with detailed and useful notes and explanatory text) appear at https://www.ali.org/ (https://www.ali.org/publications/show/data-privacy/). See also Solove, Daniel J. and Schwartz, Paul M., "ALI Data Privacy: Overview and Black Letter Text", January 24, 2020, UCLA Law Review, Vol. 68, 2020; available at SSRN: https://ssrn.com/abstract=3457563 or http://dx.doi.org/10.2139/ssrn.3457563, at p16. The text of the Principles appears from page 30 of that paper.

statement' and an ''individual notice', with two levels of individual notice, being ordinary notice and heightened notice.

The transparency statement must "clearly, conspicuously, and accurately explain the data controller or data processor's current personal-data activities". In the event that the transparency statement is changed, previous versions of the statement shall be retained and reasonably accessible. A principle of "proportionality" applies: "A transparency statement is required for both identified and identifiable personal data. The detail and sophistication of the transparency statement shall be proportionate to the magnitude of the privacy and security risks of the personal-data activities."

The individual notice is distinct from the transparency statement and must be provided in addition to the transparency statement. The notice must:

- be clear and intelligible to a reasonable person.
- inform the data subject of the nature of the data activity, the uses made of the data, the interests [of the individual that are] implicated, and how the data subject may exercise those interests,
- inform the data subject of any rights provided by applicable law that are relevant to the data activities in which the data controller is engaging.[80]

Heightened notice would be required to be given when the collection, use, or disclosure of personal data is potentially harmful to people or is significantly outside the norm.[81]

The draft Principles provide that heightened notice "shall be made more prominently than ordinary notice and closer in time to the particular data activity"[82], determined as follows:

> "For any data activity that is significantly unexpected or that poses a significant risk of causing material harm to data subjects[83], the data controller should provide reasonable "heightened notice" to affected individuals. A significantly unexpected data activity is one that a reasonable person would not expect based on the context of personal-data activities. A significant risk may exist with a low likelihood of a high-

[80] ALI, Principles of Law, Data Privacy §4(d)
[81] ALI, Principles of Law, Data Privacy §4(e), Reporter's Note 6. The ALI do not propose that consent must always be affirmative: "The form by which consent is obtained must be reasonable under the circumstances, based on the type of personal data involved, the nature of the personal-data activity, and the understandings of a reasonable data subject." However, the ALI distinguishes situations in which heightened notice is required pursuant to Principle 4(e), and here states that "only clear and affirmative consent shall suffice for valid consent. Clear and affirmative consent cannot be inferred from inaction": ALI, Principles of Law, Data Privacy §4(d).
[82] ALI, Principles of Law, Data Privacy §5(g)
[83] Assessment of the level of risks or impacts is addressed in the related paper

> magnitude injury or with a high likelihood of a low-magnitude injury. For a major potential injury, even a small likelihood may be a risk worthy of concern."[84]

Heightened notice should be more conspicuous, such as a 'pop up' that appears at the moment a data activity is about to occur. The American Law Institute's reasoning is that the timing and method of heightened notice make it more relevant to individuals, pointing out when they should be paying most attention and accordingly:

> "…heightened notice serves to lower the information burdens of mandated privacy disclosures. As Omri Ben-Shahar and Carl Schneider have noted, "[P]eople strip away information to make choices manageable". Moreover, the privacy practices of many organizations are quite similar in many respects, and basic norms of data processing have emerged, so individuals are best informed when there are practices outside the norm or practices that could potentially harm them."[85]

6.3 Requirements for (valid) consent

The OAIC's binding APP state the four key elements of consent as follows:

- the individual is adequately informed before giving consent,
- the individual gives consent voluntarily,
- the consent is current and specific,
- the individual has the capacity to understand and communicate their consent.[86]

The ACCC recommended as follows:

> that the definition of 'consent' should be updated to require a clear affirmative act that is freely given, specific, unambiguous and informed. This would amend the Privacy Act in line with the higher standard of data protection provided under the GDPR.

In particular:

- a *clear affirmative act* should be required to establish consent. This could include either ticking a website, actively selecting a setting that enables the collection of personal information, or another statement or conduct that clearly indicates the consumer's acceptance of the collection, use or disclosure of their personal information. As noted by

[84] ALI (draft) Principles of Law, Data Privacy §4(e)
[85] Solove, Daniel J. and Schwartz, Paul M. op cit, at p17, citing Ben-Shahar, Omri and Carl E. Schneider, More Than You Wanted to Know: The Failure of Mandated Disclosure, Princeton University Press, 2014
[86] OAIC, APP Guidelines, Chapter 6: APP 6 – Use or disclosure of personal information. These requirements reflect requirements as stated in many data privacy statutes: for example, GDPR Article 7 and Recital 32 provide that consents require a clear affirmative act that is freely given, specific, informed and unambiguous.

the GDPR, 'Silence, pre-ticked boxes or inactivity should not therefore constitute consent'.

- To assess whether a consent is *freely given*, it is critical that the provision of a service to the consumer must not be conditional on consent to the processing of personal information that is not necessary for the provision of that service. In addition, where electronic consents are sought, the request for consent must not unnecessarily disruptive to the use of the service for which it is provided.
- The requirement that consents must be *specific* and *unambiguous* means that consents will relate specifically to each type of data collection and must not generally be bundled. This means that, where the processing of personal information has multiple purposes, consent should be given for all of them.
- Consents must also be *informed*, to mitigate the information asymmetries between consumers and entities who are collecting their personal information.[87]

The recommendation follows now well accepted good regulatory design for requirements for consent. As noted by the ACCC, "updating consent requirements in the Privacy Act to align with the GDPR is likely to be of limited disruption to APP entities who are already following the OAIC's APP Guidelines"[88]

However, further consideration should be given to an express requirement of (objective) *intelligibility* and *reasonableness*. In this regard, the recently revised guidelines on consent[89] of the European Data Protection Board includes useful commentary and provides a number of illustrative examples:

> 5. As the WP29 stated in its Opinion 15/2011 on the definition on consent, inviting people to accept a data processing operation should be subject to rigorous requirements, since it concerns the fundamental rights of data subjects and the controller wishes to engage in a processing operation that would be unlawful without the data subject's consent. The crucial role of consent is underlined by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Furthermore, obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 of the GDPR with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is based on consent of the data subject, this

[87] ACCC, Final Report of the Digital Platforms Inquiry, pp 466-467
[88] ACCC, Final Report of the Digital Platforms Inquiry, p 467
[89] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.0 adopted on 4 May 2020

would not legitimise collection of data, which is not necessary in relation to a specified purpose of processing and be fundamentally unfair.[90]

……

Example 1: A mobile app for photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geolocalisation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.[91]

…….

Example 6a: A website provider puts into place a script that will block content from being visible except for a request to accept cookies and the information about which cookies are being set and for what purposes data will be processed. There is no possibility to access the content without clicking on the "Accept cookies" button. Since the data subject is not presented with a genuine choice, its consent is not freely given.

This does not constitute valid consent, as the provision of the service relies on the data subject clicking the "Accept cookies" button. It is not presented with a genuine choice.[92]

……

Example 7: Within the same consent request a retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies within their group. This consent is not granular as there is no separate consents for these two separate purposes, therefore the consent will not be valid. In this case, a specific consent should be collected to send the contact details to commercial partners. Such specific consent will be deemed valid for each partner (see also section 3.3.1), whose identity has been provided to the data subject at the time of the collection of his or her consent, insofar as it is sent to them for the same purpose (in this example: a marketing purpose).[93]

……..

[90] Guidelines 05/2020 on consent, page 4
[91] Guidelines 05/2020 on consent, pages 5-6
[92] Guidelines 05/2020 on consent, page 10
[93] Guidelines 05/2020 on consent, pages 11

Example 8: When downloading a lifestyle mobile app, the app asks for consent to access the phone's accelerometer. This is not necessary for the app to work, but it is useful for the controller who wishes to learn more about the movements and activity levels of its users. When the user later revokes that consent, she finds out that the app now only works to a limited extent. This is an example of detriment as meant in Recital 42, which means that consent was never validly obtained (and thus, the controller needs to delete all personal data about users' movements collected this way).

Example 9: A data subject subscribes to a fashion retailer's newsletter with general discounts. The retailer asks the data subject for consent to collect more data on shopping preferences to tailor the offers to his or her preferences based on shopping history or a questionnaire that is voluntary to fill out. When the data subject later revokes consent, he or she will receive non-personalised fashion discounts again. This does not amount to detriment as only the permissible incentive was lost.

Example 10: A fashion magazine offers readers access to buy new make-up products before the official launch.

The products will shortly be made available for sale, but readers of this magazine are offered an exclusive preview of these products. In order to enjoy this benefit, people must give their postal address and agree to subscription on the mailing list of the magazine. The postal address is necessary for shipping and the mailing list is used for sending commercial offers for products such as cosmetics or t-shirts year round.

The company explains that the data on the mailing list will only be used for sending merchandise and paper advertising by the magazine itself and is not to be shared with any other organisation.

In case the reader does not want to disclose their address for this reason, there is no detriment, as the products will be available to them anyway.[94]

Intelligibility and reasonableness are also elements of PIPEA (Canada), which provides in section 6.1:

Valid consent

6.1 For the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

[94] Guidelines 05/2020 on consent, page 12

The cross-referenced provision (clause 4.3 of Schedule 1) relevantly reads:

> 4.3.4 The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information.
>
> In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context….
>
> 4.3.5 In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.
>
> 4.3.6 The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

6.4 RECOMMENDATION 2: Clearer requirements as to consent

An example of clearer requirements as to consent is provided by clause 11 of the Personal Data Protection Bill 2019 as introduced into the Lok Sabha:

> 11. (1) The personal data shall not be processed [note that this stated prohibition is subject to a number of exceptions stated in accompanying provisions, so this prohibition is subject to important exceptions], except on the consent given by the data principal at the commencement of its processing.
>
> (2) The consent of the data principal shall not be valid, unless such consent is—
>
> (a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;
>
> (b) informed, having regard to whether the data principal has been provided with the information required under section 7;

(c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;

(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and

(e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

(3) In addition to the provisions contained in sub-section (2), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained—

(a) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal;

(b) in clear terms without recourse to inference from conduct in a context; and

(c) after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing.

(4) The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.

(5) The burden of proof that the consent has been given by the data principal for processing of the personal data under this section shall be on the data fiduciary.

(6) Where the data principal withdraws his consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such data principal.

The requirement that consent be specific and clear is addressed in characteristically blunt terms in the Brazilian data protection law:

Art. 5.XII – consent: free, informed and unambiguous manifestation whereby the data subject agrees to her/his processing of personal data for a given purpose;

Art. 8 The consent provided in Item I of Art. 7 of this Law shall be given in writing or by another means that demonstrates the manifestation of the will of the data subject.

§1 If consent is given in writing, it must appear highlighted so as to stand out from the other contractual clauses.

§2 The burden of proof is on the controller to show that consent was obtained in compliance with the provisions of this Law.

§3 It is prohibited to process personal data if the consent is defective.

§4 Consent shall refer to particular purposes, and generic authorizations for processing personal data shall be void.

§5 Consent may be revoked at any time, by express manifestation of the data subject, through a facilitated and free of charge procedure, with processing carried out under previously given consent remaining valid as long as there is no request for deletion.. .[95]

6.5 RECOMMENDATION 3: Expanding permitted general situations and permitted general situations and creating a broader category of legitimate uses

We do not recommend that the ambit of consent requirements is expanded, except perhaps for specific highly specific categories such as services specifically directed at children and vulnerable persons.

To the contrary, we suggest that the existing categories of permitted general situations[96] and permitted health situations[97] are brought within a category of 'legitimate uses', which:

- do not require notice or consent,
- must comply with the proposed additional provision addressing privacy rights and harms (see Recommendation 1 above),
- should include a broader 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),[98]
- 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),[99] and

[95] Law No. 13,709, of August 14, 2018 - Provides for the protection of personal data and changes Law No. 12,965, of April 23, 2014 (commonly referred to as the "Brazilian Internet Law")
[96] Section 16A of the Privacy Act 1988 and Chapter C of the OAIC Australian Privacy Principles Guidelines
[97] Section 16A of the Privacy Act 1988 and Chapter C of the OAIC Australian Privacy Principles Guidelines
[98] 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
[99] 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

- should include an ongoing business processes exception.

In section 3.6 of this paper, we noted how a 'legitimate interest' ground for processing could be used to 'reduce the noise' of disclosures, and potentially improve outcomes for individuals by concentrating their attention on enhanced and more prominent notice of more privacy affecting or likely unexpected acts or practices. It is probably prudent to describe this proposed exception by focussing upon its proposed content, being commonly understood ongoing businesses processes, rather than the technical and somewhat contentious interpretation of when the GDPR ground for processing is available to a data controller.[100] The oft cited concerns as to the GDPR legitimate interest ground for processing could be substantially addressed if this (proposed) business processes exception is subject to the additional requirement of this paper's (proposed) additional provision addressing privacy rights and harms (see Recommendation 1 above).

In any event, the drafting of any business processes exception will require care and consultation. By way of example, the draft IAF Fair and Open Use Act suggests an exception for "Ongoing Business Processes" as follows:

> The use is necessary to facilitate, improve, or safeguard the logistical or technical ability of the covered entity to provide goods or services to the individual, manage its operations, or protect against risk, including the use of personal data to—
>
> (A) provide, operate, or improve a specific product or service used, requested, or authorized by the individual, including the ongoing provision of customer service and support;
>
> (B) analyze the individual's use of a product or service provided by the covered entity to improve the covered entity's products, services, or operations; or
>
> (C) support basic business functions that enable a covered 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.[101]

See further the discussion in section 6.10 below.

[100] Compare in this regard the Singaporean discussion proposal outlined in section 6.10 below of this paper
[101] Definition of 'Ongoing Business Processes' at page 14, lines 401-413 of the 23 September 2019 draft of the IAF Fair and Open Use Act

6.6 RECOMMENDATION 4: Effecting privacy by default by, for example, aligning defaults with consumer preferences

Although now well accepted good regulatory design is for data privacy by default, the APPs currently do not contain requirements as to the default settings for the collection, use and disclosure of personal information.

The ACCC cited:

- market research that 85 per cent of Australian digital platforms users consider that digital platforms should only collect information needed to provide their products or services,[102] and accordingly
- suggested that "default settings enabling data processing" for a purpose other than the performance of a contract concerning the consumer should be preselected to 'off' to reflect the preference of the majority of digital platform users".[103]

The recommendation is sensible, provided that the requirement is appropriately qualified to allow defaults that reasonably enable provision of the service in the manner reasonably contemplated by the user. The ACCC does not elaborate on its qualification, but it is presumed that this is what the Commission intended by the qualifier "for a purpose other than the performance of a contract".

6.7 RECOMMENDATION 5: Additional requirements for valid consents 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
- "views that consents to collect the personal information of children by APP entities must be obtained from the child's guardian".[104]

This paper suggest that this is an excessive response to an acknowledged problem.[105]

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.

[102] Roy Morgan Research, Consumer Views and Behaviours on Digital Platforms, November 2018, p. 17
[103] ACCC, Final Report of the Digital Platforms Inquiry, p 468
[104] ACCC, Final Report of the Digital Platforms Inquiry, p 468
[105] As to the problem, see further the discussion in 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].

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.[106]

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 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.

The Californian Consumer Protection Act takes an even more detailed approach.

Under the CCPA, California consumers are afforded the right to "opt-out" of the "sale" (which is broadly defined[107]) of their personal information. "Covered Businesses" must provide notice of this right to consumers (including by providing a clear and conspicuous hyperlink entitled "Do Not Sell My Personal Information" on their websites) and must implement designated methods for consumers to opt-out (including a toll-free number and website address for opting-out). Covered Businesses must honour consumer opt-outs, and must wait 12 months before seeking re-authorization to sell their personal information.

Although such "sales" are generally not prohibited, a business that has actual knowledge that it sells the personal information of children under the age of 13 must establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent

[106] 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.

[107] Subject to various exceptions, "sell" means "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration": 1798.140. (t)(i) TITLE 1.81.5. The California Consumer Privacy Act of 2018

or guardian of that child. This affirmative authorization is in addition to any verifiable parental consent required under COPPA.

A business that has actual knowledge that it sells the personal information of minors at least 13 and less than 16 years of age must establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information. In other words, the opt-out general default is reversed to an opt-in default, in order to protect teenagers within this age bracket.

Another approach is creation of a specific no-go zone to protect children generally (although query whether the age to be specified might be less than 16). In the writer's view section 16 of the Personal Data Protection Bill 2019, as introduced into the Lok Sabha, provides a good model as to an overall principled approach, creating a specific no-go zone and appropriate carve-downs and targeting the restriction at a subset of regulated entities, being any entity that the Authority, by regulation, classify as guardian data fiduciary, because the entity operates a commercial website or online service directed at children or processes large volumes of personal data of children. The provision 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).

6.8 RECOMMENDATION 6: Reasonable accessibility by default

Most data privacy statutes do not address the particular requirements of persons with disabilities, including (but not only) in relation to the provision of privacy policies and notices at collection.

This paper suggests that reasonable accessibility by default should be a feature of a 21st century data privacy law, regardless of whether a more general right of reasonable accessibility may arise under other laws.

For example, the CCPA requires[108] privacy disclosures to be reasonably accessible to consumers with disabilities. For notices provided online, the business must follow generally recognized industry standards, such as the Web Content Accessibility Guidelines[109], version 2.1 of June 5, 2018, from the World Wide Web Consortium. In other contexts, the business must provide information on how a consumer with a disability may access the policy in an alternative format.

6.9 RECOMMENDATION 7: Improvements to transparency and intelligibility of notices at collection

Many suggestions have been made over the last decade for improvements to transparency and intelligibility of notices at collection. The principal improvements that this paper suggests are required to the Privacy Act in relation to notices at collection are:

- to narrow the focus of what must be addressed, so that what is addressed is manageable to a reader, and
- to improve transparency.

'Transparency' is used here consistently with the definition of 'transparent' in section 24(3) of the ACL, being:

(a) expressed in reasonably plain language; and

(b) legible; and

(c) presented clearly; and

[108] § 999.305 Notice at Collection of Personal Information, subsection (a)(2)(d) of Article 2, of proposed CCPA Regulations (Title 11 of the California Code of Regulations)

[109] Web Content Accessibility Guidelines, World Wide Web Consortium, Web Content Accessibility Guidelines (**WCAG**) 2.1 (June 5,2018), https://www.w3.org/TR/WCAG21/, as of 4 June 2020

(d) readily available to any party affected by the term.[110]

The CCPA Regulations provide for an additional mandatory element, being use of "a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable". The CCPA Regulations continue:

> (3) The notice at collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow:
>
> a. When a business collects consumers' personal information online, it may post a conspicuous link to the notice on the introductory page of the business's website and on all webpages where personal information is collected.
>
> b. When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.
>
> c. When a business collects consumers' personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.
>
> d. When a business collects personal information over the telephone or in person, it may provide the notice orally.
>
> (4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For 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.
>
> (5) A business shall not use a consumer's personal information for a purpose materially different than those disclosed in the notice at collection. If the business seeks to use a consumer's previously collected personal information for a purpose materially different than what was previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.

[110] See further Peter Sise, 'The Unfair Contract Term Provisions: What's Transparency Got To Do With It?', QUT Law Review, 17 (1), October 2017, pp 160–173

(6) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.

6.10 RECOMMENDATION 8: Narrower consent requirements and inclusion of legitimate uses and like provisions

The ACCC:

- recommends consumer consent to be required unless the personal information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason. These exceptions reflect the GDPR lawful bases for processing personal data on the basis of contract, legal obligation, vital interests and public task but do not include the lawful basis of 'legitimate interests';[111]
- notes that the GDPR allows for the collection of personal information on bases other than consent, and therefore this requirement is likely to involve some additional burden for digital platforms. The ACCC took into account these views in forming its final recommendations and considers it appropriate to require the basis for collecting non-essential information be consent, particularly given concerns surrounding the broad and flexible definition of the 'legitimate interests' basis for collecting personal information.[112]

This paper does not endorse the ACCC's proposals, which in the writer's view would be an excessive extension of requirements for consent, reflecting an under-valuing of legitimate uses and like provisions.

This paper has already made the following recommendations that directly relate to this topic:

RECOMMENDATION 1: Bringing privacy rights and harms explicitly into the APPs (and thereby introducing risk mitigation as a statutory element),

RECOMMENDATION 2: Clearer requirements as to consent,

RECOMMENDATION 3: Expanding permitted general situations and permitted general situations and creating a broader category of legitimate uses.

This paper further recommends that a requirement for consent should be focussed for when it is really needed, being:

[111] ACCC, Final Report of the Digital Platforms Inquiry, p 466
[112] ACCC, Final Report of the Digital Platforms Inquiry, p 489

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

Re-focussing of a requirement for consent is under active regulatory consideration in a number of comparable jurisdictions, including the Republic of Singapore. The Republic of Singapore on 14 May 2020 released a public consultation draft of a Personal Data Protection (Amendment) Bill 2020[114] and a Public Consultation Paper addressing the draft provisions[115]. The Public Consultation Paper stated the Government's intention:

- to amend the PDPA to strengthen the accountability of organisations. Accountability will be reflected as a key principle of the PDPA, and a requirement to be able to demonstrate accountability inserted into the PDPA,[116]
- to enhance the PDPA's framework for the collection, use and disclosure of personal data to enable meaningful consent where necessary. In other circumstances, organisations will be able to collect, use or disclose personal data (as applicable) for legitimate interests and business improvement purposes, especially where there are wider public or systemic benefits.[117]

Four changes to consent related provisions of the PDPA are proposed:

- expand deemed consent under section 15 of the PDPA, to include *deemed consent by contractual necessity*. Consent may be deemed to have been given for the disclosure to and use of the personal data by third-party organisations, and the third-party organisations' collection and use of the personal data, where it is reasonably necessary

[113] 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 Attachment Fourteen - American Law Institute, (draft) Principles of Law, Data Protection, Articles § 4(e)(1) and (g)(2) (conflated as "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")

[114] Consultation draft of Personal Data Protection (Amendment) Bill 2020 (a bill to amend the Personal Data Protection Act 2012 (Act 26 of 2012)

[115] Public Consultation Paper issued by The Ministry of Communications and Information and The Personal Data Protection Commission, Draft Personal Data Protection (Amendment) Bill, including Related Amendments to the Spam Control Act,14 May 2020

[116] Public Consultation Paper, paragraph 7(a), page 4

[117] Public Consultation Paper paragraph 7(b), page 4

for the conclusion or performance of a contract or transaction between an individual and an organisation.[118]

- expand deemed consent under section 15 of the PDPA, to include *deemed consent by notification*. "Consent may be deemed to be given if (i) the organisation provides appropriate notification to inform the individual of the purpose of the intended collection, use or disclosure of his/her personal data, with a reasonable period for the individual to opt-out of the collection, use or disclosure of his/her personal data for that purpose; and (ii) the individual did not opt-out within that period. 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".[119]

- by introduction of a new *legitimate interests exception*. This 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."[120]

- by introduction of a new *business improvement exception*. This exception "is intended to make clear that organisations may use personal data (that was collected in accordance with the DP Provisions) without consent for the following business improvement purposes: (i) operational efficiency and service improvements; (ii) developing or enhancing products/services; and (iii) knowing the organisation's customers. This will provide clarity for organisations to confidently harness personal data for business improvement purposes. The use of personal data for business improvement must be what a reasonable person would consider appropriate in the circumstances, and it must

[118] Public Consultation Paper, paragraph 38(a), page 12, clause 6 of the draft PDP (Amendment) Bill
[119] Public Consultation Paper, paragraph 38(b), page 12, clause 7 of the draft PDP (Amendment) Bill
[120] Public Consultation Paper, paragraph 40(a), pages 13, clause 31 of the draft PDP (Amendment) Bill

not be used to make a decision that is likely to have an adverse effect on an individual."[121]

The distinction between the two deemed consent situations and the two exceptions is that the exceptions are intended to cover situations where "larger public or systemic benefits" are such that obtaining individuals' consent may not be appropriate.[122]

The changes proposed by the Singapore Government are not fully consistent with the recommendations made in this paper, but proceed from a similar policy perspective and therefore parallel many aspects of these recommendations.

6.11 RECOMMENDATION 9: Explicit requirement for privacy by design

Assessment of risks and harms and privacy by design are now well accepted as essential features of good governance of handling of personal information by regulated entities. Recent model statutes include variants of such requirements.[123]

The Personal Data Protection Bill 2019 (India)[124], as introduced into the Lok Sabha, includes the following clauses:

> 22(1) Every data fiduciary shall prepare a privacy by design policy, containing—
>
> (a) the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal;
>
> (b) the obligations of data fiduciaries;

[121] Public Consultation Paper, paragraph 40(b), pages 13-14, clause 32 of the draft PDP (Amendment) Bill
[122] Public Consultation Paper, paragraph 40
[123] Compare Article v (Processing Risk Management) of the 23 September 2019 draft of the IAF Fair and Open Use Act and Chapter 3: Accountability and Enforcement of the ALI Principles of Law, Data Protection. As to the ALI Principles, Daniel Solove and Paul Schwartz note: "As part of achieving accountability, the Principles require an organization to develop a reasonable comprehensive privacy program. Such a program should include written privacy and security policies and procedures, personal-data inventory, risk assessment, training program, privacy and security by design, and privacy and security by default. For privacy by design, the Principles do not specify design choices. Mandating specific technological design is quite a challenging undertaking for law, and moreover, would likely face unified and strong opposition from the tech industry. Although the law probably should do more to regulate design, we were concerned about how to do this well while also being practical about not pushing U.S. law too far. The Principles, therefore, opt merely to require that "[d]esign choices and the reasoning that supports them shall be documented." Policymakers, regulators, and other actors can then evaluate these decisions. We leave it up to these parties to delve into the substance of design decisions on a case-by-case basis." Daniel J. Solove & Paul M. Schwartz, ALI Data Privacy: Overview and Black Letter Text Solove, Daniel J. and Schwartz, Paul M., ALI Data Privacy: Overview and Black Letter Text (January 24, 2020) at p27
[124] http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf. See Attachment Twelve to this paper

(c) the technology used in the processing of personal data is in accordance with commercially accepted or certified standards;

(d) the legitimate interests of businesses including any innovation is achieved without compromising privacy interests;

(e) the protection of privacy throughout processing from the point of collection to deletion of personal data;

(f) the processing of personal data in a transparent manner; and

(g) the interest of the data principal is accounted for at every stage of processing of personal data.

23. (1) Every data fiduciary shall take necessary steps to maintain transparency in processing personal data and shall make the following information available in such form and manner as may be specified by regulations—

(a) the categories of personal data generally collected and the manner of such collection;

(b) the purposes for which personal data is generally processed;

(c) any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm;

(d) the existence of and the procedure for exercise of rights of data principal under Chapter V and any related contact details for the same;

(e) the right of data principal to file complaint against the data fiduciary to the Authority;

(f) where applicable, any rating in the form of a data trust score that may be accorded to the data fiduciary under sub-section (5) of section 29;

(g) where applicable, information regarding cross-border transfers of personal data that the data fiduciary generally carries out; and

(h) any other information as may be specified by regulations.

The provision would effect a sensible balance between promoting demonstrable accountability of regulated entities (by ensuring that they effect privacy by design, but not requiring publication of that policy), and simplifying (and creating flexibility as to) the requirements of a (published) privacy policy.

7 More specific and limited reforms

In earlier sections of this paper we have suggested a number of more substantial reforms that might be considered to the Privacy Act 1988.

We now address, by way of less desirable alternative to the recommendations made above, a number of more limited recommendations as to possible changes.

Note that some of the following recommendations are themselves alternatives from other recommendations: this is a menu of options, not an all or nothing proposal.

7.1 RECOMMENDATION 10: Authority to add an additional categories of "sensitive information" (by regulation or determination of the Australian Information Commissioner)

The definition of "sensitive information" in section 6 of the Act be amended 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

7.2 RECOMMENDATION 11: Authority to direct inclusion of additional information in Privacy Policies of APP entities (by determination of the Australian Information Commissioner)

APP 1.4 be amended by inclusion of a new paragraph h, to read as follows:

such other information as the Australian Information Commissioner may by written direction specify as required to be included within an APP privacy policy, during the period that such written direction is stated to operate.

7.3 RECOMMENDATION 12: Authority to direct inclusion of additional material in privacy notice at or near time of collection(by determination of the Australian Information Commissioner)

APP 5.2 be amended by inclusion of a new paragraph (k), to read as follows:

such other matters as the Australian Information Commissioner may by written direction specify as required to be included within a notification made for the purposes of subclause 5.1, during the period that such written direction is stated to operate.

7.4 RECOMMENDATION 13: Additional requirements for privacy notices at or near time of collection (by amendment of APP 5.3)

Add a new APP 5.3 as follows:

(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.* [125]

7.5 RECOMMENDATION 14: Requirement for additional clarity and transparency as to indirect collections (viz. other than from the affected individual) (by amendment of APP 5.2(b)

Amend APP 5.2(b) by addition of the following text:

…and types or groupings of persons or entities from which a business collects personal information about the individual, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity.

7.6 RECOMMENDATION 15: Requirement for APP entities to maintain an audit and verification trail for privacy policies, privacy notices and forms of consent over time

The Privacy Act be amended to provide that:

[125] 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".

an APP entity should retain reasonable records as to the publication of a privacy policy, provision of notice and obtaining of consent by the APP entity from time to time, including reasonable records as to the form at any particular time within the records retention period of privacy policy or policies, privacy notice or notices, and consent or consents, then in use.

The records retention period could be aligned:

- for organisations, to the period required under the Corporations Act for retention of general corporate documents,
- for Commonwealth government agencies, to the period required under the Archives Act for retention of official records.

This would ensure availability of an 'audit trail' as to the form and content of disclosures, the form and content of requests for consent, and consents obtained from affected individuals in response to requests for consent in a particular form, over time.

7.7 RECOMMENDATION 16: Explicit requirements as to consent (clear affirmative act of an affected individual that is freely given, specific, unambiguous and informed)

The Privacy Act be amended to require that:

where consent is required, and subject to such exceptions from requirements to provide consent as are provided in the Act, consent requires a clear affirmative act of an affected individual that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent).

7.8 RECOMMENDATION 17: Guidelines or directions of Australian Information Commissioner may modify application of APPs in and to a specified class of circumstances as specified in that guideline or direction (but not generally)

The guidance related functions of the Australian Information Commissioner under s 28(1) of the Privacy Act 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 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 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.

The reference to a specified class of circumstances as specified in a guideline or direction is intended to ensure that the power cannot be used to change generally the operation of the APPs, but is intended to ensure operation of APPs to be modified to address particular circumstances.

7.9 RECOMMENDATION 18: When APP entities must obtain express consent

The Privacy Act (including APP 6) be amended to provide that, subject to such exceptions from requirements to provide consent as are provided in the Act:

APP entities must obtain express consent when:

(a) the personal information being collected, used or disclosed is sensitive information about an individual,

(b) the collection, use or disclosure of personal information about an individual is outside of the reasonable expectations of the individual,

(c) handling of the personal information by a regulated entity or any recipient of information derived from that personal information that the APP entity ought reasonably consider likely to receive that information, creates a significant residual risk of outputs or outcomes that cause or contribute to significant harm to an individual, taking into account all relevant circumstances including controls and safeguards implemented by an APP entity to mitigate known or reasonably anticipated risks; or

(d) an APP entity, having conducted an impact assessment and acting reasonably and with reasonable transparency, is unable to conclude with a reasonable degree of certainty that the specific collection, use or disclosure of personal information about an individual, alone or in combination with other data, produces a material, objective, and identifiable benefit for the individual or society.

The concept of derived information as referred to in paragraph (c) is intended to include certain profiling information. Consider in this regard the proposed definitions in clause 1 of the Personal Data Protection Bill 2019 (India):

> (28) "personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;
>
> (32) "profiling" means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a data principal.

7.10 RECOMMENDATION 19: When APP entities are not required to obtain express consent

The Privacy Act (including APP 6) be amended to provide

that 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.*

Attachment One - References

Acquisti, Alessandro, 'The Economics of Personal Data and Privacy: 30 Years After the OECD Privacy Guidelines', Organisation for Economic Co-operation and Development (OECD), 2010

Barocas, Solon & Helen Nissenbaum, 'On Notice: The Trouble with Notice and Consent', in Proceedings of the Engaging Data Forum: The First International Forum On The Application And Management Of Personal Electronic Information (2009)

Ben-Shahar, Omri and Carl E. Schneider, More Than You Wanted to Know: The Failure of Mandated Disclosure, Princeton University Press, 2014

Bruening, Paula J., and Mary J. Culnan, 'Through a Glass Darkly: From Privacy Notices to Effective Transparency', North Carolina Journal of Law and Technology 17, no. 4 (May 2016), p66

Calo, M. Ryan, 'Against Notice Skepticism in Privacy (and Elsewhere)', Notre Dame Law Review 87, no. 3 (2012), 1027

Cate, Fred H., 'The Failure of Fair Information Practice Principles' (2006). Consumer Protection in the Age of the Information Economy, 2006. Available at SSRN: https://ssrn.com/abstract=1156972

Cate, Fred H., and Viktor Mayer-Schonberger, "Notice and consent in a world of Big Data", International Data Privacy Law, 2013, Vol. 3, No. 2, p67

Ciocchetti, Corey A, 'The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices', The John Marshall Journal of Information Technology & Privacy Law 26, no. 1 (2008), p47

Cohen, Julie, 'What is Privacy For', (2013) 126 Harvard Law Review 1904

Cranor, Lorrie Faith, "Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice", Journal on Telecommunications and High Technology Law 10, no. 2 (2012), p36

Cudd A.E., Navin M.C. (2018), 'Introduction: Conceptualizing Privacy Harms and Values', in Cudd A., Navin M. (eds) Core Concepts and Contemporary Issues in Privacy. AMINTAPHIL: The Philosophical Foundations of Law and Justice, vol 8. Springer, Cham

Edwards, L. and M. Veale (2019). 'Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for' (2019) 16 Duke Law and Technology Review 18, pp. 16- 84

European Parliament (Policy Department for Economic, Scientific and Quality of Life Policies), New aspects and challenges in consumer protection: Digital services and artificial intelligence, April 2020, available at http://www.europarl.europa.eu/supporting-analyses

Gellman, Robert, 'Fair Information Practices: A Basic History', Version 2.19, October 7, 2019, https://bobgellman.com/rg-docs/rg-FIPshistory.pdf

Gindin, Susan E., 'Nobody Reads Your Privacy Policy or Online Contract: Lessons Learned and Questions Raised by the FTC's Action against Sears', Northwestern Journal of Technology and Intellectual Property 1:8, 2009-2010

Global Privacy Assembly (formerly International Conference of Data Protection and Privacy Commissioners), 'International Resolution On Privacy As A Fundamental Human Right And Precondition For Exercising Other Fundamental Rights', 41st International Conference of Data Protection and Privacy Commissioners 21-24 October 2019, Tirana, Albania

Gratton, Eloise, 'Beyond Consent-based Privacy Protection', July 11, 2016, submission to the Office of the Privacy Commissioner of Canada, as part of its Consultation and Call for Submissions on consent and privacy, available at https://www.eloisegratton.com/files/sites/4/2016/07/Gratton_Beyond-Consent-based-Privacy-Protection_-July2016.pdf

Hartzog, Woodrow and Solove, Daniel J., 'The Scope and Potential of FTC Data Protection' (November 1, 2015). 83 George Washington Law Review 2230 (2015); GWU Law School Public Law Research Paper No. 2014-40; GWU Legal Studies Research Paper No. 2014-40. Available at SSRN: https://ssrn.com/abstract=2461096

Johnston, Anna, 'Re-thinking transparency: If notice and consent is broken, what now?', Salinger Privacy blog post, 29 May 2020

Kaminski, Margot E. & Gianclaudio Malgieri, Algorithmic Impact Assessments Under the GDPR: Producing Multi-layered Explanations (Univ. of Colo. Law, Legal Studies Research Paper No. 19-28, 2019)

Karegar, Farzaneh, John Sören Pettersson and Simone Fischer-Hübner, 'The Dilemma of User Engagement in Privacy Notices: Effects of Interaction Modes and Habituation on User Attention', ACM Trans. Priv. Secur., Vol. 23, No. 1 (February 2020)

Kemp, Katharine, 'Concealed Data Practices and Competition Law: Why Privacy Matters', [2019] UNSWLRS 53

Kleinig, John, 'The Nature of Consent', in The Ethics of Consent- Theory and Practice (Alan Wertheimer and Franklin Miller (eds.), Oxford University Press, 2009)

Leonard, Peter, 'Big Data: Understanding and Analysing its Competitive Effects', in Competition Policy International and Melbourne Law School, Dynamic Competition in Dynamic Markets; the Path Forward, April 2019

Leonard, Peter, 'Thinking harder about data 'ownership' and regulation of data driven business', UK Society for Computers and the Law Journal, July 2019; Privacy Law Bulletin 16/3, 2019

Leonard, Peter, 'Jobs Half Done: Getting Smart about Smartphones', Computers and Law (UK Society for Computers and the Law), December 2019

Leonard, Peter, 'Data Ownership and the Regulation of Data Driven Businesses', Scitech Lawyer (American Bar Association), 16/2, Winter 2020

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, Iss 2, pp 141-181

Manwaring, Kayleen, 'Emerging Information Technologies: Challenges for Consumers' (April 25, 2017), Oxford University Commonwealth Law Journal (2017) Vol. 17 (2) (published online 17 Aug 2017); UNSW Law Research Paper No. 17-25; UNSW Business School Research Paper. Available at SSRN: https://ssrn.com/abstract=2958514

Mcdonald, Aleecia M., and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies', I/S: A Journal of Law and Policy for the Information Society 4, no. 3 (2008), p26

Moerel, Lokke, 'EU Data Protection Laws Are Not Fit For Purpose: They Undermine the Very Autonomy of the Individuals They Set Out to Protect', Morrison & Foerster blog post 21 May 2020

Moerel, E.M.L. and Prins, J.E.J. (Corien), 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (May 25, 2016). Available at SSRN: https://ssrn.com/abstract=2784123 or http://dx.doi.org/10.2139/ssrn.2784123

Nissenbaum, Helen, 'A Contextual Approach to Privacy Online', Daedalus 140, no. 4, 29 September 2011, pp32–48. doi:10.1162/DAED_a_00113

Nissenbaum, Helen, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford, CA, Stanford Law Books, 2010

Norton, Thomas B, 'The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model', (2016) 27 Fordham Intellectual Property, Media and Entertainment Law Journal 181,

Ohlhausen, Maureen K and Alexander P Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy', (2015) 80 Antitrust Law Journal 121

Ohm, Paul, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', 57 UCLA L. REV. 1701 (2010)

Ohm, Paul, 'Changing the Rules: General Principles for Data Use and Analysis', in Lane, Julia I., Privacy, big data, and the public good : frameworks for engagement, New York: Cambridge University Press (2014), pp96-111

Reidenberg, Joel R., N. Cameron Russell, Alexander Callen, Sophia Qasir, and Thomas Norton, 'Privacy Harms and the Effectiveness of the Notice and Choice Framework', 11(2) Journal of Law and Policy for the Information Society (2015)

Schaub, Florian, Rebecca Balebako, and Lorrie Faith Cranor, 'Designing Effective Privacy Notices and Controls', IEEE Internet Computing, June 16, 2017, 1–1. doi:10.1109/MIC.2017.265102930

Schermer, B.M. et al, 'The crisis of consent: how stronger legal protection may lead to weaker consent in data protection', (2014) 16(2) Ethics and Information Technology

Schwartz, Paul M. & Daniel J. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', (2011) 86 N.Y.U. L. REV. 1814

Schwartz, Paul M & Karl-Nikolaus Peifer, Transatlantic Data Privacy Law, (2017) 106 GEO. L.J. 115

Schwartz, Paul M., 'Global Data Privacy: The EU Way', (2019) 94 N.Y.U. L. REV. 771, 772-73

Sise, Peter, 'The Unfair Contract Term Provisions: What's Transparency Got To Do With It?', QUT Law Review, 17 (1), October 2017, pp 160–173

Sloan, Robert H. and Warner, Richard, 'Beyond Notice and Choice: Privacy, Norms, and Consent' (March 25, 2013). Chicago-Kent College of Law Research Paper No. 2013-16, available at SSRN: https://ssrn.com/abstract=2239099 or http://dx.doi.org/10.2139/ssrn.2239099

Sinha, Amber and Scott Mason, 'A Critique of Consent in Information Privacy', The Centre for Internet and Society Blog, 11 January, 2016, https://cis-india.org/internet-governance/blog/a-critique-of-consent-in-information-privacy

Sokol, D. Daniel and Roisin Comerford, 'Antitrust and Regulating Big Data' (2016) 23 George Mason Law Review 1130

Solove, Daniel J, 'Conceptualising Privacy', (2002) 90 California Law Review 1087

Solove, Daniel J, “Privacy Self-Management and the Consent Dilemma”, Harvard Law Review 126 (2013), pp880–903, https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/

Solove, Daniel J. and Schwartz, Paul M., ‘ALI Data Privacy: Overview and Black Letter Text’ (January 24, 2020), UCLA Law Review, Vol. 68, 2020. Available at SSRN: https://ssrn.com/abstract=3457563 or http://dx.doi.org/10.2139/ssrn.3457563

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

Waldman, Ari Ezra, ‘Privacy, Notice, and Design’, Stanford Technology Law Review 21, no. 1 (2018): 129–84

Wachter, S. and B. Mittelstadt. ‘A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI’, (2019) Columbia Business Law Review 2, pp. 1–130

Zanfir-Fortuna, Gabriela, ‘Forgetting About Consent: Why the Focus Should Be on 'Suitable Safeguards' in Data Protection Law’ (May 2013), available at SSRN: https://ssrn.com/abstract=2261973 or http://dx.doi.org/10.2139/ssrn.2261973