Privacy Harms

A paper for the Office of the Australian Information Commissioner

Peter G Leonard

June 2020

Table of Contents

Privacy Harms

A paper for the Office of the Australian Information Commissioner

Peter Leonard[1]

PART A – SCOPE AND RECOMMENDATIONS

1 Scope

This paper (entitled *Privacy Harms*) was commissioned by the Office for the Australian Information Commissioner together with a companion paper entitled *Notice, Consent and Accountability: addressing the balance between privacy self-management and organisational accountability*.

For convenience of reference, we will call this paper the *Harms Paper* and the accompanying paper the *Self-Management Paper*.

Each paper is intended to stand alone, although there is close complementarity of subject matter coverage in the two papers.

The Self-Management Paper concludes with 19 recommendations for consideration in any review of the Privacy Act 1988. Recommendations 2, and 4 through 19, of the Self-Management Paper) address specific improvements to the notice and consent framework as that framework is currently implemented in the Australian Privacy Principles. A subset of those recommendations (Recommendations 10 through 19 in the Self-Management Paper) are expressed as possible alternative reforms.

The Self-Management Paper concludes that improvements to the notice and consent framework (as suggested in Recommendations 2 and 4 through 19 in the Self-Management Paper) should not be considered in and of themselves as effective regulatory control of data privacy, given:

[1] 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. The views expressed in this review report are those of the author not those of any of those other bodies and organisations.

- 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 Self-Management Paper concluded that 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. The Self-Management Paper expresses the opinion that 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 the Self-Management Paper addresses a possible reform to effect a legislated requirement for APP entities to act reasonably to assess, mitigate and manage residual data privacy risks (remaining after proper mitigation) of significant privacy harms to affected individuals.

Recommendation 4 (Effecting privacy by default) of the Self-Management Paper also addresses reduction of risk of privacy harms to affected individuals through improved processes within APP entities.

The Self-Management Paper highlights 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, the Self-Management Paper contends that:

- 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; and
- data privacy by design and default and responsible data minimisation will remain laudatory design principles consistent with good implementation of the Australian Privacy Principles, but not an essential element of the Australian Privacy Principles.

Of course, legislating a requirement for APP entities to identify and mitigate significant privacy harms would requires clear specification of harms that are privacy harms and how APP entities should assess and manage risk of such harms.

Accordingly, the central focus of this paper is:

- identification of risks and harms that are privacy risks and harms; and
- specification of processes and practices that APP entities should adopt to assess, mitigate and manage risk and impact.

2 Key recommendations

This paper makes six recommendations:

Recommendation 1: The Privacy Act should expressly address the meaning of interference with the privacy of an individual

Recommendation 2: APP entities should be required to demonstrate accountability to affected individuals, through introduction into the Privacy Act 1988 of a legislated requirement for APP entities to conduct a comprehensive privacy program and to meet a new legislated standard of care

Recommendation 3: Privacy harms should be identified in the Privacy Act 1988 by a non-exhaustive (illustrative) list

Recommendation 4: Regulatory requirements in Australia should reflect good global regulatory practice, but Australia should not be a front-runner

Recommendation 5: Privacy impact assessments should be expressly recognised in the Privacy Act 1988

Recommendation 6: Having regard to the accountability requirements elsewhere recommended in this paper and the Self-Management Paper (as below referred to), this paper does not recommend that the conduct of privacy impact assessments is specifically mandated, or that the Act specify thresholds for when a privacy impact assessment should be considered (preliminary risk assessment) or conducted (level of risk threshold assessment)

The context of these recommendations is explained in Section 3 below.

3 This paper and the terms of reference

3.1 Previously stated views of the OAIC

In developing recommendations made in this Harms Paper and in the Self-Management Paper, the author has taken into account publicly stated views of the OAIC, including the following:

Striking the right balance – organisational accountability

To get the balance right, the OAIC supports increased accountability for APP entities. including:

- *Requirements to embed privacy into the design of technologies, architecture and systems*
- *Mandatory privacy impact assessments for high risk data practices*
- *The introduction of an enforceable privacy code for designated digital platforms*
- *Enhanced ability for individuals to require their data to be erased, unless there is an overriding reason for the information to be retained. This should be complemented by a right for individuals to object to the handling of their personal information for specific purposes*
- *Introduction of a third-party certification scheme to provide assurance to consumers about privacy credentials*
- *Higher penalties for privacy infringements and new powers for Australians to take legal action in case of breach of their privacy.*

The OAIC also suggests a prohibition on unreasonable personal information handling practices and a new requirement to use and disclose personal data 'fairly and lawfully'. This may involve the introduction of 'no-go zones' which specify certain information-handling practices that will generally be considered inappropriate, irrespective of whether consent has been received.

The author considers that the recommendations made in this Harms Paper and in the Self-Management Paper are broadly consistent with those views. Of course, the recommendations in these papers are those of the author alone, and do not in any way represent the views of the OAIC.

3.2 Terms of Reference for these papers and the responses in these papers

(a) Privacy and privacy harms in the digital age

The author was provided by the OAIC with Terms of Reference to scope this Harms Paper and the Self-Management Paper.

The individual papers were structured by the author to collectively address these Terms Of Reference, but to do so in a way which facilitates understanding of the reasoning underlying the author's analysis.

This section 3.3 is intended to assist correlation of the discussion in the two papers to the Terms of Reference.

Relevant Terms of Reference *appear below in italics*.

An objective of the Privacy Act is to promote the protection of the privacy of individuals. In the report 'For Your Information: Australian Privacy Law and Practice', the Australian Law Reform Commission stated that '[a]lthough the right to privacy is an individual right, there is a strong public interest in protecting that right'.[2] *Similarly, Chief Justice Gleeson of the High Court of Australia has observed that while there is a 'lack of precision of the concept of privacy', the 'foundation of much of what is protected, where rights of privacy, as distinct from rights of property, are acknowledged, is human dignity'.*[3]

- *Historically, what have privacy laws tried to protect? What are the current harms to individuals that Australia's privacy framework should protect against? How has this changed in the digital age? Do these align with contemporary community expectations?*

Section 6 of this Harms Paper addresses *what is privacy* and *a privacy harm*.

We conclude that data privacy regulation should protect both individual interests and societal[4] (collective) rights or interests.

The nature of those rights or interests, and how they are given effect in the current provisions of the Privacy Act 1988, are discussed in Part C (in particular, section 4) of the Self-Management Paper.

The Self-Management Paper includes a recommendation as to how an individual 's right not to be subject to privacy harms could be better tied to the Australian Privacy Principles: see Recommendation 1 (Bringing privacy rights and harms explicitly into the APPs) of the Self-Management Paper, which is in the form of a composite provision to supplement the APPs.

In the Self-Management Paper (in particular at section 4.2), we also note the weakness of the link between the operative provisions of the Privacy Act 1988 and the stated purpose and objects of the Act.

That weakness is further considered in section 5 (Constraints of the existing statutory framework of the Privacy Act 1988) of this Harms Paper, leading to Recommendations 1 and 3 of this Harms Paper.

[2] Australian Law Reform Commission 2010 'For Your Information: Australian Privacy Law and Practice' <https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/5-the-privacy-act-name-structure-and-objects/the-objects-of-the-act/> , Chapter 5, paragraph 5.123

[3] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63, [41] & [43]

[4] As to societal interests, see further footnote 67 in the Self-Management Paper and accompanying text.

- *Should Australia's privacy framework seek to protect group or collective privacy?*[5] *If so, what are the collective harms that may result from breaches of privacy?*

Only in terms of recognition of collective interests of individuals, and not a separately defined societal interest in data privacy.

Consideration of societal harms (e.g. loss of social trust) requires difficult judgements concerning the definition, identification and concreteness of such harms. This leads to concern as to whether regulated entities are well placed to assess them. Although consideration of societal harms may be relevant, there does need to be criteria and proxies for such societal harms that are objective and measurable. Given these complexities, this paper does not endorse inclusion of societal harms as a separate privacy harm, but does suggest that the evaluative criteria which a regulated entity is required to apply should include "whether the [proposed] 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)".[6]

See further section 6.5 (How data privacy interests and 'harms to privacy' fit together) of this Harms Paper.

- *How can legislative reform practically address individual and collective privacy harms?*

See our specific recommendations in both papers, and in particular Recommendations 1 and 3 in the Self-Management Paper, and !, 2 and 3 of this Harms Paper.

- *Are these issues considered in any other jurisdictions? If so, what have been the practical operation and implications in these jurisdictions?*

International comparisons are made throughout each paper.

Recommendation 1 (Bringing privacy rights and harms explicitly into the APPs) at section 4.3 of the Self-Management Paper has been significantly influenced by the Canadian Privacy Commissioner's discussion as to fair and responsible handling of personal information, but also address some deficiencies in the current provisions of Canadian data privacy laws.

- *Is the language of privacy 'harms' still appropriate and useful in the digital age? Does the language of 'harm' imply that an act or practice is only wrong or illegal if it has direct or known consequences for an individual? Is there a threshold expectation that any breach of privacy is a 'harm', regardless of whether a consequential harm flows from the breach?*

Yes. The relevance of a privacy harms has increased as the diversity of uses and applications of digital data has increased and APP entities have acquired greater capability to understand

[5] See for example the discussion of 'group privacy' in Taylor, L, Floridi, L, van der Sloot, B (2017) Group Privacy: New Challenges of Data Technologies, 1st ed. New York, NY: Springer.
[6] See the draft composite paper at Recommendation 1 of the Self-Management Paper, in particular paragraph (c)(vi).

and address (including through automated individuation) known or inferred interests or attributes of individuals.

See in particular section 6 of this Harms Paper.

(b) Rights and prohibitions in the Privacy Act

The OAIC is considering whether it would be appropriate for the Privacy Act to set out rights for individuals and prohibitions on the processing of personal information in certain circumstances.

The OAIC has recommended that several privacy rights be incorporated into Australia's privacy framework, including a right of erasure, right to object and rights in relation to automated decision-making, that may be modelled on similar rights in the GDPR.

The OAIC has also recommended introducing 'no-go zones' and the requirement that information be used and disclosed fairly and lawfully into the Privacy Act.

In relation to the introduction of rights for individuals into the Privacy Act:

- *What are the strengths and weaknesses of this rights-based approach?*

The Self-Management Paper examines why rights of individuals as to notices and consents need to be supplemented by more specific and direct restrictions as to what APP entities may do in the course of handling of personal information.

The nature of those restrictions is specifically addressed by:

See our specific recommendations:

  - Recommendation 1 (Bringing privacy rights and harms explicitly into the APPs) of the Self-Management Paper; and
  - Recommendation 2 (APP entities should be required to demonstrate accountability to affected individuals, through introduction into the Privacy Act 1988 of a legislated requirement for APP entities to conduct a comprehensive privacy program and to meet a new legislated standard of care) of this Harms Paper.

- *In addition to the right of erasure, right to object and rights in relation to automated decision-making, are there any rights from the GDPR that may be appropriate in an Australian context?*

Recommendation 1 (Bringing privacy rights and harms explicitly into the APPs) of the Self-Management Paper, in the form of a composite provision to supplement the APPs, addresses fairness and transparency without the ambiguities and uncertainties which are inherent in Article 22 of the GDPR.

We also make a number of specific transparency recommendations (see Recommendations 2 to 19 in the Self-Management Paper.

If our Recommendation 1 of the Self-Management Paper as to a composite provision to supplement the APPs was accepted:

- We consider that this provision would address the relevant concern and accordingly do not consider that 'data minimisation', as expressed in Article 5(1)(c) of the GDPR, would significantly add to this provision read together with APP 3.1, APP3.2, APP 6.1 and APP 6.2;
- We consider that this recommendation would address the relevant concern and do not consider that 'the purpose limitation, as expressed in Article 5(1)(b) of the GDPR, would provide significant benefit.

- *Are there any other privacy rights that may be appropriate to introduce into the Privacy Act?*

Not as a 'right', but rather:

- clarity as to the link between rights and operative provisions,
- a composite provision to supplement the APPs and link the operation of the APPs to consideration of harms (Recommendation 1 of the Self-Management Paper), and
- a clear articulation of *privacy harms*.

Data protection regulation, both in Australia under the Privacy Act and internationally, typically draws on core data protection principles set out in the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[7] *Several of these data protection principles are expressly defined in article 5 of the GDPR (such as the purpose limitation and data minimisation principles).*[8]

- *What are the strengths and weaknesses of expressly defining these privacy principles into the Privacy Act?*

See above.

- *Would it be appropriate to model the definitions of these principles on the GDPR?*

[7] Organisation for Economic Co-operation and Development (OECD) 1980, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>.

[8] These principles are reflected in the OAIC's guidance. See for example OAIC 2019, Australian Privacy Principles guidelines: Chapter B: Key Concepts <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/#primary-purpose-and-secondary-purpose> which reflects the purpose limitation principle at paragraphs B.98-B.99 and OAIC 2019, Australian Privacy Principles guidelines: Chapter 3: APP 3 – Collection of solicited personal information <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information/> which reflects the data minimisation principle at paragraphs 3.13 – 3.19

No, because we consider that the statement of principles in the GDPR:

- is not particularly clear (the principles depend heavily upon interpretation of lengthy and complex recitals and background materials)
- would not readily translate into the Australian regulatory environment (given that there is no general human rights statute in Australia).
- *Are there any other principles that may be appropriate to expressly define in the Privacy Act?*

See above.

The Canadian privacy framework includes a broadly defined prohibition (which requires organisations to only handle personal information in a manner that a reasonable person would consider appropriate), which is given further particularity by the Canadian Privacy Commissioner (in the form of several 'no-go zones' for the processing of personal information).

- *What are the strengths and weaknesses of including these types of prohibitions on the handling of personal information in the Privacy Act?*

See our discussion of the no-go zones proposed in Canada in section 4.2 (Is privacy as a fundamental right relevant to applying the APPs?) of the Self-Management Paper.

In fact, many of Canadian self-described 'no-go zones' might more accurately be described as high risk or high alert zones, as the relevant act or practice there described is not absolutely prohibited.

We consider that acts or practices involving use of personal information to create individuated effects or outcomes upon individuals which have significant risk of harms to those individuals should be specifically regulated, regardless of whether the individuated effect or outcome involves a direct use of personal information about an individual or is enabled through pseudonymisation processes which do not directly include use or disclosure of personal information about individuals.

We commend that consideration is given to creation of a no-go zone in relation to profiling of children.

- *What are the strengths and weaknesses of the approach in Canadian privacy law to broadly defining prohibitions and include additional particularisation in Commissioner guidance?*

Our Recommendation 1 of the Self-Management Paper, in the form of a composite provision to supplement the APPs, addresses fairness and takes into account weaknesses of the Canadian model (including weaknesses identified by the OPC).

Similar, a number of our recommendations 2 to 19 in the Self-Management Paper takes into account learnings from the Canadian model.

- *What are the strengths and weaknesses of including more proscriptive prohibitions on information handling directly in the Privacy Act (for example, by specifically legislating no-go zones)?*

  See above.

- *What prohibitions should be introduced into the Privacy Act?*

See above.

Another model proposed in the UK is a statutory duty of care on companies to protect users from online harms (which notably excluded harms resulting directly from a breach of data protection legislation).[9] *The UK Joint Committee on Human Rights disagreed with this approach, proposing that this statutory duty of care should include a requirement for companies to adhere to robust standards on how people's data is processed*.[10]

- *What are the strengths and weaknesses of introducing a statutory duty of care on APP entities into the Privacy Act?*

See section 6.5 (How data privacy interests and 'harms to privacy' fit together) and our Recommendation 2 of this Harms Paper.

As there stated, this paper commends creating accountability by:

- requiring APP entities to design and implement a comprehensive privacy program to identify, mitigate and manage residual risks of privacy harms to affected individuals arising from collection, use and disclosure of personal information about those affected individuals, and
- creation of a standard of care that is related to particular factors, of which design and implementation of a comprehensive privacy program is a key component (the nature and scope of the program should take into account the size of the entity and the level of privacy risks associated with collection and handling of personal information by the entity).

The regulatory objective should be to create appropriate regulatory incentive for good data privacy practice by regulated entities.

[9] HM Government 2019, Online Harms White Paper <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf>

[10] UK Joint Committee on Human Rights 2019, The Right to Privacy (Article 8) and the Digital Revolution <https://publications.parliament.uk/pa/jt201920/jtselect/jtrights/122/122.pdf>

The regulator should be given appropriate direction and enforcement powers, and capabilities, to ensure that these proposed obligations are given effect.

If the regulator is given these powers and capabilities, we do not suggest that a private right of action is conferred upon affected individuals.

- *What would be the content of such a duty of care?*

See section 6.5 (How data privacy interests and 'harms to privacy' fit together) and our Recommendation 2 of this Harms Paper.

- *Would such a duty of care complement, or be introduced instead of, the privacy rights, principles and/or prohibitions considered above?*

The duty of care would complement the privacy rights, principles and/or prohibitions as recommended elsewhere in this Harms Paper and the Self-Management Paper.

PART B – REVISING THE PRIVACY ACT 1988 TO ADDRESS PRIVACY HARMS

4 Principles for good regulatory design

4.1 Scoping our discussion in this paper

As stated by the OECD Policy Secretariat:

> The dramatic opportunities enabled by changes in technologies and global flows have also raised new challenges and concerns for individuals, organisations, and society with respect to the protection of privacy. There is a general perception that certain risks associated with privacy have increased as a result of the shift in scale and volume of personal data flows and the ability to store data indefinitely. These changes, along with the evolving role of individuals and the increasing economic value of personal data, give rise to concerns related to the security of personal data, unanticipated uses, monitoring and trust. The result is a privacy environment that is challenging for organisations and individuals to navigate.[11]

This paper considers the scope of privacy harms that are addressed by the Privacy Act 1988 (C'th) and how the scope might be better defined, or changed, to better address concerns of Australian citizens.

This examination requires us to engage with two key concepts:

- what is *privacy*, and
- what is *a privacy harm*?

The two concepts are closely intertwined. This paper will conclude (as some other studies on this topic have done) that protection of legitimate privacy rights and interests of individuals requires an approach that combines:

- 'top-down'(what is privacy?), and
- bottom-up (what harms are we seeking to avoid or mitigate and manage?).

This conclusion does not lead us to a crisp definition of data privacy. Alas, one conclusion of this paper is that the search for crisp statutory definitions of privacy and privacy harm respectively is a search for a chimera. This conclusion explains why almost all data privacy statutes refer to *a right of individuals in and to (data) privacy*, and to be *protected against (data) privacy harms*, without telling us much more about what privacy and a privacy harm actually mean.

[11] OECD, The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines, at section 2.4. Privacy risks in the evolving environment (p37)

4.2 Relevant propositions outside scope of review in this paper

A number of propositions should not be controversial and are therefore not further explored in this paper:

(a) The Privacy Act 1988 addresses only a subset of the set of rights of privacy of individuals as commonly asserted and as referred to in international conventions and declarations of human rights. The Privacy Act could be more accurately described as an *Information* Privacy Act.

(b) The Privacy Act 1988 does not address many forms of surveillance and intrusion.

(c) Pervasive or otherwise overly intrusive surveillance (even when implemented *without* facial recognition or without other identification of individuals) is regarded by many Australian citizens as an unreasonable invasion of personal privacy.

(d) Ongoing discussion of a need for a new tort or statutory cause of action for serious invasion of privacy is an indication of the limited scope and coverage of the Privacy Act 1988.

(e) Even within that limited ambit, the definitions of "personal information" and "collection" (for inclusion in a "record" or "generally available publication"), and the wide ranging exceptions and exemptions within the Privacy Act 1988, further reduce ambit of operation of the statute. The Privacy Act 1988 only addresses information or an opinion about an identifiable individual as collected and held in some tangible form.

(f) There is general agreement among data privacy experts, and endorsement by many data protection regulators, that privacy analysis and enforcement should be more risk based.[12]

[12] Eduardo Ustaran CIPP/E, Partner of Hogan Lovells, recently commented that "Perhaps the greatest success of the GDPR so far has been the introduction of the risk-based approach to compliance and regulatory action. Data is all around us, and its protection is a responsibility that needs constant recalibration. A static and prescriptive law would have been incapable of addressing the nuances of the digital economy. Fortunately, the GDPR is not that. The GDPR has flexibility and common sense at its core, and thanks to that, we should regard it as a framework that can adapt to the privacy and cybersecurity needs of our challenging world.": IAPP, The GDPR at Two: Expert Perspectives. See further Martin Abrams, Privacy Law Must Focus on Consequential Harm, Information Accountability Foundation blog post of 2 June 2020, https://informationaccountability.org/2020/06/privacy-law-must-focus-on-consequential-harm/; Lynn Goldstein and other IAF authors, Bermuda Report on Information Accountability: Prepared by the Information Accountability Foundation for the Office of the Privacy Commissioner for Bermuda 28 March 2020, https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/f70f79_199e97af7ae640adbc10cd07eba34470-2.pdf; Privacy Risk Management White Papers and associated materials of the Centre for Information Policy Leadership (**CIPL**) as available at 'Privacy Risk Management' https://www.informationpolicycentre.com/privacy-risk-management.html# and

(g) The Privacy Act 1988 does not today address the range of individuated outcomes upon individuals (or small cohorts of individuals) that adversely impact legitimate interests of those individuals, or that are otherwise unexplained or inexplicable to those individuals, in circumstances where the algorithms and data used to create automated outputs that are used to effect those outcomes did not use personally identifying information about those individuals. Such data and algorithm enabled individuated outcomes are in this paper called (for convenience) *algorithmic effects upon individuals*.[13]

(h) In relation to an algorithmic effect upon an individual enabled through the use of non-identifying personal information about that individual, this outcome is out of scope of operation of the Australian Privacy Principles, and accordingly may be caused by an act or practice of an APP entity regardless of whether this individuated outcomes is harmful to an individual. (Note, however, that some individuated outcomes are effected upon an individual through the use of identifying personal information about that individual: such use (and associated collections or disclosures) of personal information is already regulated by the Privacy Act.)

(i) There are many harms that individuals may suffer from invasions of privacy that are not addressed by the Privacy Act 1988. Some of these harms are addressed by other statutes. Various sector specific statutes regulate uses of data about individuals in those sectors. Consumer protection laws, including laws as to misleading and deceptive conduct, unconscionable conduct and unfair contract terms, address certain relevant harms. Competition laws address some harms to the long-term interests of consumers caused by anti-competitive acts and practices of businesses.

4.3 Principles of good regulatory design

Our discussion as to *what is privacy* and as to *privacy harms* leads us to consideration of good regulatory design. Regulatory forms can be placed on a continuum of government oversight ranging from self-regulation, through quasi-regulation and co-regulation, to direct government regulation:

- *Self-regulation* is generally characterised by industry-formulated rules and codes of conduct, with industry solely responsible for enforcement.

particularly CIPL, What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework: Report of the CIPL Accountability Mapping Project, May 2020

[13] This paper avoids use of the word 'profiling' as that term has become closely associated with the narrower and more technical operation of Article 22 of the GDPR. As to use of 'profiling' more generally, see 35th International Conference of Data Protection and Privacy Commissioners 23-26 September 2013, Warsaw, Resolution on Profiling, available at http://globalprivacyassembly.org/wp-content/uploads/2015/02/Profiling-resolution2.pdf

- *Quasi-regulation* describes those arrangements where government influences businesses to comply, but which do not form part of explicit government regulation.
- *Co-regulation* typically refers to situations where industry develops and administers its own arrangements, but government provides legislative backing to enable the arrangements to be enforced.
- *Direct government regulation* comprises primary and subordinate legislation.[14]

Commonwealth data privacy regulation has been principally by statute, with subordinate legislation playing a limited role. The Australian Information Commissioner has constrained authority to promulgate legally binding instruments.

Where data privacy concerns overlap with concerns addressed by other areas of regulation and other regulators, a question arises as to:

- which legislative instrument appropriately addresses what subject matter and harms, and
- which regulator has the appropriate skills, experience and authority to address that subject matter and harms.

Good regulatory design requires identification of:

- overlaps in current coverage of regulation
- overlaps in current allocation of responsibilities between regulators,
- gaps in coverage of subject matter and harms.

There is significant overlap between other statutes and the Privacy Act 1988. For example, in *Australian Competition And Consumer Commission v Google Australia Pty Ltd & Anor* NSD1760/2019 the ACCC alleges that Google represented to users of the Android Operating System that it would not obtain data about their location, or that where such data was obtained it would only be used for the user's own purposes, but that Google did obtain and retain such data and used that data for Google's purposes. This practice was alleged to contravene provisions of Australian Consumer Law (**ACL**), relevantly including:

[14] Council of Australian Governments (COAG), Best Practice Regulation: A Guide for Ministerial Councils and National Standard Setting Bodies, October 2007, https://www.pmc.gov.au/sites/default/files/publications/COAG_best_practice_guide_2007.pdf. See also As to good regulatory design in Australia, see Commonwealth of Australia, The Australian Government Guide to Regulation, 2014, https://www.pmc.gov.au/sites/default/files/publications/Australian_Government_Guide_to_Regulation.pdf; Council of Australian Governments (COAG), Best Practice Regulation: A Guide for Ministerial Councils and National Standard Setting Bodies, October 2007, https://www.pmc.gov.au/sites/default/files/publications/COAG_best_practice_guide_2007.pdf

(a) engaging in conduct this is misleading or deceptive or likely to mislead or deceive, in contravention of s 18 of the ACL;

(b) making false or misleading representations that the Android OS, Google Services or Pixel phones have performance characteristics, uses or benefits that they did not have, in contravention of s 29(1)(g) of the ACL; and

(c) engaging in conduct that was liable to mislead the public as to the nature, the characteristics and the suitability for purpose of the Android OS, Google Services or Pixel phones, in contravention of s 33 or, alternatively, s 34 of the ACL.[15]

The alleged harms to users included:

(a) the misleading information provided by Google means that Users were not able to make an informed choice about the Personal Data in relation to their location that they wished Google to obtain and use;

(b) if Users had been able to make an informed choice, they may have taken steps to stop Google obtaining and retaining the Personal Data in relation to their location;

(c) the private information of many Users - the Personal Data in relation to their location - has been obtained, retained and used by Google (including for its own purposes) without those Users' knowledge.[16]

This paper notes that these alleged practices are:

- within the scope of coverage of the Australian Privacy Principles,
- within the regulatory remit of the Australian Privacy Commissioner, and
- alleged to cause harms readily characterised as privacy harms.

Overlap between coverage of the Privacy Act 1988 and of other statutes need not of itself be a concern.

However, where there is overlap, it is important that there is clarity, either through statutory design or as a matter of inter-agency practice, as to which regulator is responsible for overseeing particular subject matter and addressing particular harms.

[15] Concise Statement dated 29 October 2019, Part C: Primary Legal Grounds For The Relief Sought, paragraphs [60]-[63].
[16] Concise Statement dated 29 October 2019, Part D: Alleged Harm Suffered, paragraphs [64]-[65]

A recent example of an inter-agency initiative to address less than clear statutory allocation of responsibilities is the ACCC/OAIC statement on *Compliance and Enforcement Policy for the Consumer Data Right*.[17]

A recent example of the harms that may be effected upon individuals as a result of unclear allocation of regulatory responsibilities is afforded by the release of passengers from the COVID-19 affected Ruby Princess.[18]

Where we identify reasonably likely harms to individuals through uses of data and that these harms are not adequately addressed by current provisions of the Privacy Act 1988 or other statutes, or the current state of judge-made law, this paper suggests that we should ask the question:

> *Is this harm, either by its inherent nature or by the nature of the skills or processes or good practices required to reliably identify and address the harm, more appropriately addressed*
>
> - *as a privacy harm, and then by a privacy statute, or*
> - *through another existing legal or human rights paradigm, or*
> - *through another, entirely new legal constructs (such as a law that specifically addresses algorithmic effects upon individuals).*

It follows that characterisation of a harm (as a data privacy harm or something else) should not be an arid, academic, debate: this characterisation is necessary for good regulatory design.

4.4 Applying the principles of good regulatory design to privacy harms

In summary:

- Overlap in coverage creates risks both for related entities and for regulators, of over-regulation, under-regulation, or inconsistent regulation, but does not necessarily lead to these poor outcomes.
- A more significant risk of poor outcomes arises from gaps in coverage of existing regulatory coverage that leave unregulated circumstances that are reasonably likely to

[17] ACCC/OAIC Compliance and Enforcement Policy for the Consumer Data Right, V1, May 2020, https://www.accc.gov.au/system/files/CDR%20-%20CE%20-%20Joint%20ACCC%20and%20OAIC%20compliance%20and%20enforcement%20policy%20-%208%20May%202020.pdf, and Guidance for Policymakers available at https://www.pmc.gov.au/regulation/guidance-policymakers

[18] See further the Terms of Reference for The Special Commission of Inquiry into the Ruby Princess, at https://www.rubyprincessinquiry.nsw.gov.au/

arise (notwithstanding market forces) where unacceptable harms may be experienced by citizens.

The first question in addressing gaps in regulatory coverage spaces should be:

(1) *Is the harm sufficient in impact and sufficiently non-transitory in nature that it should be addressed through regulation?*

The second question should be:

(2) *Is regulation the best way to address that harm?*

Are there other incentives or disincentives that may be used to change behaviour of relevant entities: social opprobrium, media focus, education as to risks and harm litigation, and so on?

Where regulation is determined to be the best way to address that harm, a third question should be:

(3) *What is the most effective and sustainable form of regulation?*

Regulation as to process and allocation of accountability and responsibility will usually be the most sustainable form of regulation:

- in industry sectors that are unpredictably evolving and rapidly changing,
- in industry sectors with complex or highly fragmented supply ecosystems, or
- for applications with highly variable and context specific risk profiles.

Hard coded prohibitions will often be more effective at addressing a known harm, largely because the prohibition is readily understood by regulated entities and therefore more readily self-applied. An example of a hard-coded prohibition is proposed clause 16(5) of the Personal Data Protection Bill 2019 of India, which is currently before the Lok Sabha:

> The guardian data fiduciary shall be barred from profiling, tracking or behaviourally monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child.

Hard coded prohibitions are useful for addressing more egregious harms and where the nature of the harm can be relatively durably described. However, many privacy affecting uses and applications of data and advanced technology have some or all of the characteristics described above, where it is difficult to draft a provision of stable and predictable operation and impact over time.

4.5 Regulation as to process and allocation of accountability and responsibility

For this reason, regulation as to process and allocation of accountability and responsibility is likely to be a key component of data privacy regulation for the foreseeable future.

Regulation as to process and allocation of accountability and responsibility may be directly specified by the regulator, or imposed through requirement for industry sectors to comply with codes of conduct or practice which specify process and allocate accountability and responsibility. These codes may be subject to regulatory review and assessment as a pre-condition to promulgation.

Regulation that imposes obligations upon entities to undertake processes or procedures (such as risk assessment, mitigation and management) must also take into account the question of whether compliance management systems in practice reduce the likelihood of noncompliance.[19]

Regulation as to process and allocation of accountability and responsibility requires clarity, through legislated or regulator-provided specification, as to:

(1) *What are the processes that should be specified?*

(2) *Which entity is responsible to apply a specified process?*

(3) *Whether the entity is responsible for applying the process to assess, manage and mitigate risks in relation to only its own activities, or is responsible for that assessment across a broader data or provider ecosystem (i.e. end-to-end data management and including acts of an affected individual).*

(4) *Whether the entity is accountable and liable if other persons in the data or provider ecosystem enabled by the regulated entity create unacceptable risks or harms.*

(5) *The threshold of risk or potential impact at which a particular process is required to be applied. Different thresholds may apply at different levels of risk or impacts, and if that threshold is crossed, require application of different form (frameworks, methodologies or tools) or intensity of process.*

Sections 5 and 6 of this paper address the above issues.

[19] The issue of where compliance management systems reduce the likelihood of noncompliance arses across the variety of domains where compliance management systems have either become a legislated requirement or accepted industry practice, including environment, workplace health and safety, finance, health care, and aviation. For a recent empirical study, see Coglianese, Cary and Nash, Jennifer, 'Compliance Management Systems: Do They Make a Difference?' (May 7, 2020), in Cambridge Handbook of Compliance (D. Daniel Sokol & Benjamin van Rooij eds., Cambridge University Press, forthcoming)

However, the discussion of how to address these issues needs to be grounded in a clear understanding of:

- what can be done within the existing statutory framework of the Privacy Act 1988 (as discussed in section 5), and
- what is *privacy* and *a privacy harm* (as discussed in section 5).

5 Constraints of the existing statutory framework of the Privacy Act 1988

The Privacy Act 1988 addresses certain act and practices of APP entities: most relevantly, but not only, collection, use or disclosure of personal information about an individual collected for inclusion in a record or a generally available publication.

5.1 Privacy, privacy risks and privacy harms and the current Privacy Act 1988

New readers of the Privacy Act 1988 are often surprised that the statute does not define "privacy" or the circumstances in which an act or practice is to be taken to cause harm to an individual.

The Overview in Schedule 1 - Australian Privacy Principles states that Part 1 of the APPs (APP 1 and AAP 2) "sets out principles that *require APP entities to consider the privacy of personal information*, including ensuring that APP entities manage personal information in an open and transparent way". However, the APPs do not state how APP entities should determine the circumstances in which rights or interests of individuals in and to privacy are affected, or how to evaluated the nature or extent of harm to those rights or interests for the purpose of application of the APPs.

Most operative provisions in the Privacy Act 1988 use *privacy* as an adjective (occasionally an adverb) in a description of something else: privacy *policy*, Privacy *Act*, *Australian* Privacy *Principle*, privacy *authorities* and so on. (We note in passing that the objects provision, section 2A, uses *privacy* as a concept in and of itself. Section 2A is considered in detail in the next section of this paper. However, it is not an operative provision.)

A rare exception is APP 12.3, which states:

> If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:
>
> (a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
>
> (b) *giving access would have an unreasonable impact on the privacy of other individuals*; ….

However, APP12.3 does not state what *privacy* is, or how to assess *impact on the privacy of other individuals*, or how to assess whether that impact is reasonable or *unreasonable*.

The Privacy Act 1988 does not generally use *risk* or *harm* as operative concepts.

"Risk" is used in the Act in two ways that are not relevant to this paper: first, in the sense of insurance risks and credit risks, and second, in the concept of individuals who are *at risk* from an eligible data breach. In other words, it is not used in the two senses relevant to this paper, being:

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

"Harm" is used in the Act only in (or in relation to) *Part IIIC Notification of eligible data breaches* of the Act, in the context of a breach being an eligible data breach where, relevantly, "a *reasonable person* would conclude that the access or disclosure would be *likely to result* in *serious harm to any of the individuals to whom the information relates*".[20]

In the context of determining whether a data breach is notifiable, the Act informs an APP entity as to relevant matters to have regard to in determining whether access or disclosure would be likely, or would not be likely, to *result in serious harm*.[21]

The Explanatory Memorandum informs us that "the 'reasonable person' and 'likely risk' elements of the notification standard, by using commonly-understood legal standards of objectivity and probability, are intended to provide greater certainty for regulated entities while maintaining consistency with the core element of the ALRC recommendation" (of a 'real risk of serious harm' standard)[22].

The Explanatory Memorandum also informs us that:

> Serious harm, in this context, could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach. Though individuals may be distressed or otherwise upset at an unauthorised access to or unauthorised disclosure or loss of their personal information, this would not itself be sufficient to require notification unless a reasonable person in the entity's position would consider that the likely consequences for those individuals would constitute a form of serious harm.[23]

[20] Section 26WF(2)
[21] Section 26WG
[22] Explanatory Memorandum to the Privacy Amendment (Notifiable Data Breaches) Bill 2016, paragraph [8]
[23] Explanatory Memorandum to the Privacy Amendment (Notifiable Data Breaches) Bill 2016, paragraph [9]

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

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

Section 13 states:

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

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

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

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

personally identifying information about individuals.

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

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

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

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

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

- what individuals might reasonably be expected to know or indeed require as an inherent attribute of a particular activity of an APP entity (being an activity that the affected individual wants the APP entity to do),
- reasonable expectations of affected individuals,
- "reasonableness" or "fairness" as used an objective standard (in the tort of negligence and in many other areas of law).

Although Australian privacy regulators and privacy professionals often talk about 'privacy risk management' and 'privacy impact assessment', the Privacy Act 1988 does not describe what is a *privacy risk*, what is a *privacy impact*, what is *an appropriate process for risk or impact assessment, mitigation or management*, or (to take a more specific example) what is *the relevance or otherwise of controls and safeguards* implemented by an APP entity in relation to the handling of personal information.

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

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

None of these concepts appear relevant in Australia from a plain reading of the Privacy Act 1988. Unless, of course, privacy risk, harm and impact assessment are concepts legally relevant to interpretation and operation of the APPs through the statements of purpose and objects of the Privacy Act 1988.

5.2 Purpose and objects of the Privacy Act 1988

Section 2A of the Privacy Act 1988 set 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 tied to the operative provisions of the Act. Indeed, the Act as enacted did not include this statement of objects. Section 2A was included in the Act only in 2012.

On a plain reading of the APPs, it is reasonable to ask whether the stated objects of the Privacy Act have any relevance in interpretation of the APPs, and accordingly whether any broader scope of data privacy rights of individuals is relevant in application of the APPs.

If the Parliament did not consider it necessary to define privacy as a right of individuals and instead elected to describe what APP entities must do, and not do, in relation to personal information about individuals, why is a diffuse concept of *privacy* relevant at all to an APP entity in making a decision as to its handling of personal information that it, as its discretion elects to collect? Or to put it another way, so long as an entity complies with the letter of the APPs and other operative provisions and therefore does not do anything within the apparently exhaustive and prescriptive list of acts or practices that are *an interference with the privacy of an individual*, why should the APP entity legally concern itself with *what privacy is*, or *what is a privacy harm*?

Of course, in working out the meaning of any provision of the Privacy Act (including the APPs), where multiple interpretations are possible, the interpretation that promotes the purpose or objects of the Act is to be preferred.[24] However, the issue of multiple interpretations generally does not arise in interpretation of the APPs.

The Privacy Act might have been would be expressly stated to be beneficial legislation that should be interpreted in a way that is beneficial to those who it is designed to help: the affected individuals.[25] However, as stated by the Full Federal Court in *AIT18 v Australian Information Commissioner* [2018] FCAFC 192 at [85]:

> …the Privacy Act itself reflects the Parliament's concern to recognise and protect individual privacy within the framework of a complex statutory regime. It does so by a series of statutory provisions which protect the privacy of individuals from unlawful or arbitrary interference but also by specifying circumstances (or "exceptions") which reflect the Parliament's concern to strike an appropriate balance between competing

[24] Section 15AA of the Acts Interpretation Act 1901 (Cth). See further Australian Law Reform Commission, For Your Information: Australian Privacy Law And Practice (ALRC Report 108) at Chapter 5 (The Privacy Act: Name, Structure and Objects), particularly [5.90]-[5.130]

[25] Jurecek v Director, Transport Safety Victoria [2016] VSC 285 [24] and Harrison v Victorian Building Authority (Human Rights) [2015] VCAT 1791 [16], applying s.32(1) of the Victorian Charter of Human Rights and Responsibilities Act 2006 (the Charter). See further Office of the Victorian Information Commissioner, Key Concepts, November 2019. Of course, these is no analogous legislation to the Victorian Charter of Human Rights and Responsibilities Act 2006 at the Commonwealth level.

> community interests. We accept the Information Commissioner's submission that, in those circumstances, the exceptions should be interpreted carefully so as to preserve the balance which the legislation strikes between the competing community interests, noting also the relevance of the fact that Art 17(1) ICCPR is not expressed in unqualified terms. It does not confer an absolute "right to privacy", but rather creates a right not to be subjected to arbitrary or unlawful interference with one's privacy. The exceptions in the Privacy Act reflect the Parliament's identification of circumstances in which interference with a person's privacy is not arbitrary or unlawful.

The Court continued (at 88]:

> It may be accepted that, as a statement of general principle, legislation such as the Privacy Act should, **as far as the statutory language permits**, be construed so as to give effect to Australia's international obligations (see, for example, *NBGM v Minister for Immigration and Multicultural Affairs* [2006] HCA 54; 231 CLR 52 at [61] per Callinan, Heydon and Crennan JJ and *Minister for Immigration and Multicultural and Indigenous Affairs v QAAH of 2004* [2006] HCA 53; 231 CLR 1 at [34] per Gummow ACJ, Callinan, Heydon and Crennan JJ). But the words of qualification which are set out immediately above are critical.[26]

In interpreting the statutory language in section 2A, it is difficult to reconcile the first two stated objects: to *promote the protection of the privacy of individuals*; and to recognise that *the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities*.

Does this mean that although the protection of the privacy of individuals is intended to be promoted by the Act, and therefore the Act is intended to be interpreted beneficially to interests of affected individuals, that beneficial interpretation must be balanced with the interests of entities in carrying out their functions or activities? A reasonable contention is that if the Parliament had intended primacy of privacy of individuals over interests of entities in carrying out their functions or activities, the Parliament could have so stated, or could have stated privacy as a *right* of individuals to be balanced against *interests* (not a right) of entities in carrying out their functions or activities.

Nor did the Parliament expressly recognise any *societal interests* in protection of the privacy of individuals. This leaves open an interpretation of the Act that each individual can freely and readily bargain away (through choice following notice, whether or not that choice is

[26] See also Coco v the Queen [1994] HCA 15; (1994) 179 CLR 427; Jeremy Lee v Superior Wood Pty Ltd (01 May 2019) [2019] FWCFB 2946; 286 IR 368 (Deputy President Sams, Deputy President Gostencnik, Commissioner McKinnon)

expressed in the form of an affirmative consent) their individual data privacy, without invoking any societal interest in protection of the privacy of individuals.

The closest that the stated objects come to addressing accountability of regulated entities is the statement of object in paragraph (d) of section 2A:

to promote responsible and transparent handling of personal information by entities,

as read together with the overview statement in Schedule 1 that, the APPs 1 and 2 set out:

principles that require APP entities to consider the privacy of personal information, including ensuring that APP entities manage personal information in an open and transparent way.

However, this is a reading of "objects" and an "overview", each not operative provisions.

Unlike the objects in section 2A, the preamble to the Privacy Act 1988 has been in the Act from its first enactment. The preamble recites that Australia is a party to the International Covenant on Civil and Political Rights (**ICCPR**) and has undertaken to adopt such legislative measures as may be necessary to give effect to the right of persons not to be subjected to arbitrary interference with their privacy, home or correspondence. The preamble also recites that the Council of the Organisation for Economic Co-operation and Development has recommended that member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines annexed to the recommendation (the **OECD Privacy Guidelines**). It recites that Australia has informed the Organisation that it will participate in the recommendation concerning those Guidelines.

Do these references assist interpretation of the Privacy Act 1988?

In *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 Kenny and Edelman JJ stated (at [69] and [70]):

> …the right of privacy in Art 17 of the ICCPR is not defined. Its content is not prescribed. Different state parties to the ICCPR have given different content to its terms. The same breadth of approach is taken in the Guidelines which provide (at [41]) that:
>
> > The terms "personal data" and "data subject" serve to underscore that the Guidelines are concerned with physical persons. The precise dividing line between personal data in the sense of information relating to identified or identifiable individuals and anonymous data may be difficult to draw and must be left to the regulation of each Member country. In principle, personal data convey information which by direct (e.g. a civil registration number) or indirect linkages (e.g. an address) may be connected to a particular physical person.

In *Purvis v New South Wales* [2003] HCA 62; (2003) 217 CLR 92, 156 [206], Gummow, Hayne, and Heydon JJ said of the use of international instruments and legislation from other jurisdictions in relation to disability discrimination:

> Considerable care must be taken, therefore, before applying what has been said about either the aims or the effect of other forms of disability discrimination legislation from other jurisdictions to the construction of the Act. Even more care must be taken before adopting the necessarily general forms of aspirational, as distinct from normative, statements found in international instruments as an aid to resolving the particular questions of construction which now arise. Aspirational statements are commonly concerned to state goals, not to identify the particular methods by which the stated goals will be achieved. Those international instruments to which we were referred took this aspirational form.

Accordingly, the objective of promoting "responsible" handling of personal information by entities is difficult to give substantive operation as the Act currently stands.

The objective of promoting "transparent" handling of personal information is easier to apply, as the APPs are quite explicit as to what must be stated within privacy policies and notices at collection. However, even this objective is somewhat opaque. Transparency as a regulatory concept cannot be assessed without answering to two questions: *transparent to whom*, and *transparent for what purpose*?

Under Australian Consumer Law, a term in a consumer contract or a small business contract is "transparent" if the term is expressed in reasonably clear language, legible, presented clearly and readily available to any party affected by the term.[27] This takes a particular, buyer protection, perspective of ensuring that consumers and small business are appropriately informed in the making of buying decisions.

The GDPR also appears to treat "transparency" as a data subject-centric construct[28], although the A29WP Guidance[29] also references accountability:

> "transparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights ".

[27] ACL section 24(3)
[28] Article 5(1)(a)
[29] Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

As Peter Cullen of the Information Accountability Foundation notes[30], in data privacy policy there is conflation of accountability (of the regulated entity) and control (through choice by the data subject) within an object of transparency. Peter Cullen uses two examples to illustrate that "the complexity of technology and associated data flows and uses is becoming simply too difficult" to meet a simple objective of transparency *to affected individuals*:

> In the case of AdTech, the complexity of players and data flows and by extension "explainability", is perceived to inhibit the ability of individuals to exercise their right to object to receiving an ad or the profiling necessary to deliver the ad. Regulators believe that the processes are so complex and the descriptions so obtuse that individuals are not knowledgeable enough to exercise their rights. This criticism not only bundles the objective of transparency with legal requirements, as noted above, but it also suggests an objective of transparency is "verifiability".
>
> ….
>
> In Artificial Intelligence (AI), transparency is increasingly subsumed by "interpretability". As highlighted in their paper Toward Trustworthy AI Development[31], the authors note "AI systems are frequently termed "black boxes" due to the perceived difficulty of understanding and anticipating their behaviour. This lack of interpretability in AI systems has raised concerns about using AI models in high stakes decision-making contexts where human welfare may be compromised. Having a better understanding of how the internal processes within these systems work can help proactively anticipate points of failure, audit model behaviour, and inspire approaches for new systems."[32] But this lack of understanding actually raises a different objective of transparency other than being able to explain what is going on. It suggests in addition to helping people understand the reasons for doing the processing and the means to achieve those objectives, transparency and interpretability help achieve "verifiability".

5.3 Connecting operative provisions to the statements of purpose and objects in the Privacy Act

To summarise the analysis in the preceding section of this paper:

[30] Peter Cullen, Transparency Needs a Makeover, Information Accountability Foundation blog of 5 May 2020, available at https://informationaccountability.org/2020/05/transparency-needs-a-makeover/

[31] Brundage, Miles and others, Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims, April 2020, arXiv:2004.07213 (Cornell University), https://arxiv.org/pdf/2004.07213.pdf. See further Price II, William Nicholson and Rai, Arti Kaur, Clearing Opacity through Machine Learning (February 12, 2020). 106 Iowa L. Rev. (Forthcoming); http://dx.doi.org/10.2139/ssrn.3536983

[32] Ibid (Brundage, Miles and others)

- The purpose and objects stated in the Privacy Act 1988 are useful guides as to the intended operation of the Act.
- However, on the current state of the law and principles of Australian statutory interpretation, these statements of purpose and objects are unlikely to significantly affect legal interpretation of the operative provisions as to those listed circumstances in which an act or practice is an invasion of privacy of an individual.
- As used in the Privacy Act 1988, the concept of transparency is neither adequately explained not connected back to its other role (in addition to openness to affected individuals) of enabling verifiability (and therefore accountability) of regulated entity as to a regulated entity's acts and practices.

5.4 RECOMMENDATION 1: The Privacy Act should expressly address the meaning of interference with the privacy of an individual

It is unfortunate that the concepts of:

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

are not expressly operative concepts within the APPs, and therefore are not relevant considerations in determining whether and when there is an *interference with the privacy of an individual.*

This paper recommends that any review of the Privacy Act 1988 should address these deficiencies.

Note that this recommendation is closely related to Recommendation 1 (Bringing privacy rights and harms explicitly into the APPs) in section 4.3 of the Self-Management Paper, which addresses a possible reform to effect a legislated requirement for APP entities to act reasonably to assess, mitigate and manage residual data privacy risks (remaining after proper mitigation) of significant privacy harms to affected individuals.

6 What is privacy and a privacy harm?

6.1 Privacy in international instruments

''Privacy" is protected under various international instruments, including the United Nations Declaration of Human Rights 1948 and (as noted in the preamble to the Privacy Act 1988 as discussed above) the United Nations International Convention on Civil and Political Rights 1966 (**ICCPR**).[33] 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 OECD Privacy Guidelines[34] as revised in 2013 relevantly state:

> 2. These Guidelines apply to personal data, whether in the public or private sectors, *which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties*.
>
> 3. The principles in these Guidelines are complementary and should be read as a whole. They should not be interpreted:
>
> a) as preventing the application of different protective measures to different categories of personal data, depending upon their nature and the context in which they are collected, stored, processed or disseminated; or
>
> b) in a manner which unduly limits the freedom of expression.
>
> 4. Exceptions to these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:
>
> a) as few as possible, and

[33] See also 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, at http://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf

[34] Before the 2013 revision, OECD, Annex to the Recommendation of the Council of 23rd September 1980: Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, available at https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part3; as revised in 2013, OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013), available at https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

b) made known to the public.

5. In the particular case of federal countries the observance of these Guidelines may be affected by the division of powers in the federation.

6. These Guidelines should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact transborder flows of personal data.

The OECD Guidelines also noted "that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information".

The policy basis for the OECD Guidelines was stated in the Explanatory Memorandum to the Guidelines as follows:

> The remedies under discussion are principally safeguards for the individual which will prevent an invasion of privacy in the classical sense, i.e. abuse or disclosure of intimate personal data; but other, more or less closely related needs for protection have become apparent. Obligations of record-keepers to inform the general public about activities concerned with the processing of data, and rights of data subjects to have data relating to them supplemented or amended, are two random examples. Generally speaking, there has been a tendency to broaden the traditional concept of privacy ("the right to be left alone") and to identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.[35]

More specifically, the Explanatory Memorandum to the OECD Privacy Guidelines stated:

> The approaches to protection of privacy and individual liberties adopted by the various [OECD member] countries have many common features. Thus, it is possible to identify certain basic interests or values which are commonly considered to be elementary components of the area of protection. Some core principles of this type are: setting limits to the collection of personal data in accordance with the objectives of the data collector and similar criteria; restricting the usage of data to conform with openly specified purposes; creating facilities for individuals to learn of the existence and contents of data and have data corrected; and the identification of parties who are responsible for compliance with the relevant privacy protection rules and decisions. Generally speaking, statutes to protect privacy and individual liberties in relation to personal data attempt to cover the successive stages of the cycle beginning

[35] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Explanatory Memorandum, paragraph 2.

> with the initial collection of data and ending with erasure or similar measures, and to ensure to the greatest possible extent individual awareness, participation and control.[36]

Some Australian human rights statutes also recognise privacy as a basic human right. For example, section 13 of the Charter of Human Rights and Responsibilities Act 2006 (Vic) provides:

> Privacy and reputation: A person has the right— (a) not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with.

Section 12 of the Human Rights Act 2004 (ACT) and section 25 of the Human Rights Act 2019 (Qld) are in almost identical terms.

While these statutes include "privacy" in the list of rights that they accord the status of a 'human right', the statutes do not define the term, or assist in determining how and to what extent the privacy right intertwines with other freedoms, rights and interests.

6.2 What is 'privacy'?

Privacy is commonly described in a general way as t*he interests a person has in controlling what others know about them, in being left alone and in being free from interference or intrusion: the 'right to be let alone'*.[37] This formulation expands upon the Warren and Brandeis (1890) summation of privacy as the 'right to be let alone'[38] and focusses upon the seclusion and separation elements of privacy.

In the Canadian Supreme Court case of *Vickery v Nova Scotia Supreme Court (Prothonotary)*, Cory J described "privacy" as a right which:

> ….inheres in the basic dignity of the individual. This right is of intrinsic importance to the fulfilment of each person, both individually and as a member of society. Without privacy it is difficult for an individual to possess and retain a sense of self-worth or to maintain an independence of spirit and thought.[39]

Each of these formulations state a right or interest of a breadth of operation that can only be aspirational in our information economy. In any event, this right or interest must be considered together with countervailing societal and organisational interests, whatever

[36] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Explanatory Memorandum, paragraph 5.
[37] See further Cohen, Julie, 'What is Privacy For', (2013) 126 Harvard Law Review 1904; Nissenbaum, Helen, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford, CA, Stanford Law Books, 2010; Colin J Bennett, 'In Defence of Privacy: The concept and the regime', (2011) 8 Surveillance and Society 485
[38] Warren, Samuel and Louis Brandeis, "The Right to Privacy", (1890) Harvard Law Review 193
[39] Vickery v. Nova Scotia Supreme Court (Prothonotary), [1991] 1 S.C.R. 671, available at https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/738/index.do, as later applied in Jones v. Tsige, 2012 ONCA 32

weighting is given to the respective interests (and noting that the use of the concept of "balancing of" the respective interests clearly underweights many citizens assessment of their interest in and to data privacy).

The Australian Law Reform Commission in its *For Your Information: Australian Privacy Law And Practice* report (the recommendations of which ultimately led to the objects clause being inserted into the Privacy Act),[40] expressed *what is privacy?* in this way:

> Ascertaining the scope of the legal 'right' is a more difficult task. Despite the best efforts of legal scholars, the term 'privacy' confounds attempts at delivering a universal definition. In ALRC 22, it was noted that 'the very term "privacy" is one fraught with difficulty. The concept is an elusive one'. Professor J Thomas McCarthy has noted:
>
> > It is apparent that the word 'privacy' has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts … Like the emotive word 'freedom', 'privacy' means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.[41]

Raymond Wacks, then Professor of Law and Legal Theory at the University of Hong Kong, back in 2000 colourfully described privacy regulation as follows:

> Murkiness abounds in the privacy jungle. The question of the relationship between data protection legislation and the right of privacy has long inhabited this murk. The two plainly overlap; indeed, the latter is normally invoked as the interest which animates the former. But even in our burgeoning information society, 'privacy' is not necessarily violated by what we once called 'data banks'.[42]

Professor Daniel J. Solove has described privacy as a "conceptual jungle" and a "concept in disarray". "[T]he attempt to locate the 'essential' or 'core' characteristics of privacy has led to failure".[43] Professor Woodrow Hartzog has stated that "Privacy has really ceased to be helpful as a term to guide policy in the United States, because privacy means so many different things to so many different people."[44]

---

[40] See page 217 of the Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012, referencing ALRC Recommendation 5-4

[41] Australian Law Reform Commission, For Your Information: Australian Privacy Law And Practice (ALRC Report 108, August 2010) at Chapter 1, under sub-heading 'The meaning of privacy', [1.31] – [1.68], quoting .J McCarthy, The Rights of Publicity and Privacy (2nd ed, 2005), [5.59]. See also, D Solove, 'A Taxonomy of Privacy' (2006) 154(3) University of Pennsylvania Law Review 477, 479

[42] Raymond Wacks, "What has data protection to do with privacy?" (2000) 6(9) Privacy Law and Policy Reporter 143; see also Raymond Wacks, 'The Poverty of Privacy' (1980) 96 Law Quarterly Review 73

[43] Daniel J. Solove, Understanding Privacy (2008), at page 196 and at page 8 respectively

[44] Hartzog, Woodrow, "The Fight to Frame Privacy", 111 Michigan Law Review 1021 (2013)

When making its recommendation for introduction of a statutory cause of action for serious invasions of privacy in New South Wales, the NSW Law Reform Commission referred to Lord Reid's analysis in *Ridge v Baldwin*[45] to the effect that because a concept is difficult to define does not consequentially render it meaningless and unworthy of legal protection:

> To suggest that it is impossible to protect privacy generally in the manner proposed in our Bill because the concept cannot be precisely defined is to succumb to what Lord Reid once described as "the perennial fallacy that because something cannot be cut and dried or lightly weighed or measured therefore it does not exist".[46]

The Victorian Law Reform Commission's *Workplace Privacy: Issues Paper*[47] commenced from the proposition that "privacy can be expressed as a right, and that this right to privacy can then form the basis for determining what are legitimate interests in privacy". The VLRC formulated a working definition of "privacy" in terms of *what the right to privacy encompasses*, namely:

- the right not to be turned into an object or statistic, that is, the right of not to be treated as if they are things; and
- the right to establish and develop relationships with other people.[48]

The New Zealand Law Commission advocated a blended 'core values'[49] approach, which recognises 'privacy as a sub-category of two interconnected core values':

- the autonomy of humans to live a life of their choosing; and
- the equal entitlement of humans to respect ('not to be turned into an object or thing')[50]

A focussed and justly famous formulation of information privacy is that of Alan Westin:

> "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[51]

This formulation does not present data privacy necessarily as a *right*, or as a *human right* (of individual humans), or a *fundamental* human right (trumping lesser interests and rights in contract when they conflict). It is not necessary to see privacy as a right in order to

[45] Ridge v Baldwin and others [1963] 2 All ER 66
[46] NSW Law Reform Commission, Invasion of Privacy, Report 120 (April 2009), at [4.16] (page 18)
[47] Victorian Law Reform Commission, Workplace Privacy: Issues Paper (2002), https://www.lawreform.vic.gov.au/sites/default/files/IssuesPaperfinal.pdf, also citing Victorian Law Reform Commission (Kate Foord), Defining Privacy (2002), available at https://www.lawreform.vic.gov.au/sites/default/files/Defining_Privacy_Occasional_Paper.pdf
[48] ALRC, at [1.53] and [1.54]
[49] New Zealand Law Commission, Privacy Concepts and Issues: Review of the Law of Privacy Stage 1, Study Paper 19 (2008), [3.10].
[50] ALRC, at [1.54]
[51] Alan Westin, Privacy and Freedom, New York: Atheneum, 1970, p7

recognise the expectations and claims of affected persons to be legally entitled to determine (not own) when, how, and to what extent information about them is communicated.

This distinction between:

- privacy as a (fundamental) human right, and
- privacy as a value, interest or other entitlement that should be conferred by law in order to nurture digital trust or to address other societal interests,
- legitimate (reasonable) expectations of individuals as to protection of interests that they assert should ground a legal right,

is important.

Focus upon data privacy as a right risks downplaying legitimate concerns of sections of society as to how data about them is being collected and used,[52] concerns which if not addressed may undermine the societal interest in digital trust that underpins a vibrant data economy. As stated by Spiros Simitis in 1978, "privacy considerations no longer arise out of particular individual problems; rather they express conflicts affecting everyone'.[53]

It is important to recognise trust, transparency and accountability, as values in any of themselves, particularly in the dynamic data economy:

> Technological change is accompanied by trust as expectation: the expectation that the state has a duty of care and that whatever government is in office will exercise its powers and deliver the means of protecting us from new dangers. In relation to privacy and surveillance, levels of trust are vulnerable if government appears unresponsive or is deemed too slow to react to the dangers posed by the use of those technologies.[54]

Perceived data privacy risks, even if not realised, may also undermine the public confidence that is necessary for the successful adoption of new technologies.

Data privacy may also promote human dignity by protecting an individual from undue interference or harm by others. We have already noted that that algorithmic effects upon individuals may adversely impact legitimate interests of those individuals or otherwise be unexplained or inexplicable to those individuals. This is a harm to dignity and autonomy of

[52] Colin J Bennett, 'In Defence of Privacy: The concept and the regime', (2011) 8 Surveillance and Society 485
[53] Simitis, Spiros, "Reviewing Privacy in the Information Society", (1978) University of Pennsylvania Law Review 135, pp 707-746
[54] The Royal Academy of Engineering, 'Dilemmas of Privacy and Surveillance: Challenges of Technological Change' (Report, March 2007) [8.1], also cited in Queensland Law Reform Commission, Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies: Consultation Paper, December 2018, at [2.50]

individuals, regardless of whether it directly impacts any other recognised human right of individuals.

As stated by the Australian Law Reform Commission (**ALRC**), however "privacy" may be defined, it:

> …underpins:
>
> - meaningful and satisfying interpersonal relationships, including intimate and family relationships;
> - freedom of speech, thought and self-expression;
> - freedom of movement and association;
> - engagement in the democratic process;
> - freedom to engage in secure financial transactions;
> - freedom to pursue intellectual, cultural, artistic, property and physical interests; and
> - freedom from undue interference or harm by others.[55]

6.3 Categorisation of privacy and data privacy and data privacy interests

There are four main categories of privacy protected by laws in modern privacy protecting jurisdictions:[56]

- of *the person,* or *bodily privacy*—the interest in freedom from interference with an individual's physical person and bodily integrity, including from direct and indirect physical intrusions. It may also include psychological intrusion.
- of *personal space,* or *territorial privacy*—the interest in limiting intrusion into personal spaces, including in the home, workplace and in public. This concerns a person's sense of personal safety and dignity as well as their property rights.
- of *personal communications,* or *communications and surveillance privacy*—the interest in freedom from interference with personal communications, including interception, recording, monitoring or surveillance.

[55] ALRC, Serious Invasions Of Privacy In The Digital Era (ALRC Report 123), Principle 1: Privacy is a fundamental value worthy of legal protection, at para 2.6

[56] This categorisation reflects the IAPP Glossary of Privacy Terms as available at https://iapp.org/resources/glossary/#information-privacy. This categorisation adopted by the Queensland Law Reform Commission in the Commission's Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies: Consultation Paper, December 2018, at [2.7]

- of *personal information,* or *data privacy*—the interest in controlling access to, use and disclosure of information about the person, including images and information derived from analysis of other data.

As we have noted, the Privacy Act 1988 protects only *data privacy*, and then only in limited circumstances.

Of course, data may record of activities which invoke another category of privacy – for example, personal wellness devices collect data that may relevantly invoke any and all of the categories of privacy described above.

6.4 Categorisation of data privacy interests

A number of *data privacy interests* can be identified within the category of data privacy:

- privacy of *personal behaviour*, or *behavioural privacy*—the interest in freedom from undue observation of or interference with a person's activities, movements, associations and preferences, including sensitive matters such as sexual preferences, political activities and religious practices. This interest includes a particular democratic political interest - the interest of a citizen not to be observed by the state when pursuing lawful activities,
- privacy of *personal experience*— the interest of an individual in freedom from collection and use of data about an individual's personal experiences, including what an individual reads or views, and who they interact and associate with (the last limb being sometimes broken out as privacy of association,
- *locational privacy* or *tracking privacy*—the interest in controlling the extent to which information about an individual's current or past location(s) is accessed and used by others,
- privacy of *thoughts and feelings*—the interest a person has in not sharing their thoughts or feelings and not having them revealed to others,
- privacy of *attention*—the ability to exclude intrusions that force a person to direct attention to them, rather than to matters of their own choosing,
- privacy through *anonymity*—the interest in choosing to be and remain anonymous, for example, when entering into transactions with organisations.[57]

Protection of each of these interests of individuals is also a societal interest, as loss of privacy is "not only is a loss to each of us as individuals, but also impairs creativity in art, science, and living. The loss of privacy can hurt each of us and all of us".[58]

[57] Ibid. (Queensland Law Reform Commission), at [2.8], pp6-7
[58] Ibid. (Queensland Law Reform Commission), citing JL Mills, Privacy: The Lost Right (Oxford University Press, 2008) 13–22

An individual may not be able to articulate any or all of the above data privacy interests, but still consider that an intrusion by an organisation upon an individual's interest in the relevant subject matter causes harm to the individual. Perceptions of privacy harms can be very subjective and intertwined with attributes about organisations, particular classes or organisations, sectors of the economy and so on. Although extreme outliers should not be allowed to drive a policy agenda for society, the societal consensus necessary to set a reasonably stable scope of legal protection of data privacy cannot simply be determined by rule of the majority: sufficient number of citizens feel more viscerally about data privacy that their concerns need to be taken into account. Personal views of citizens about data privacy should not be discounted simply because they are not congruent with the views of rights lawyers, data ethicists, or other experts. 'Legitimate interests in privacy' may therefore be much more encompassing than a reasonable person might consider as within the realm of the private.[59]

However, giving legal protection to a broad range of subjective interests potentially creates a very wide scope of alleged harms, particularly if:

- compensable harm to an individual includes damage suffered in the nature of embarrassment, anxiety or distress[60], and
- an individual is conferred a right to bring a private right of action and to join in a class action with significant groups of like plaintiffs.

Unqualified legal protection of an individual against any intrusion by an organisation upon an individual's interest in relevant subject matter as above described could create business uncertainty and unduly impede the conduct of a vibrant democracy and information economy.

As a result, privacy interests proposed for legal protections are usually qualified by concepts such as:

- objective reasonableness, as in a 'reasonable expectation of privacy'[61], and
- by reference to additional elements of intent or impact or both, as in the proposal for a statutory cause of action for (only) invasions of privacy that are serious, committed

[59] The writer's view here expressed is directly contrary to the perspective of Judith Wagner DeCew has proposed that the "realm of the private to be whatever types of information and activities are not, according to a reasonable person in normal circumstances, the legitimate concern of others": see Judith Wagner DeCew, In Pursuit of Privacy: Law, Ethics, and the Rise of Technology (Ithaca, NY and London: Cornell University Press, 1997) and the further discussion in Adam Moore, Defining Privacy, Journal Of Social Philosophy, Vol. 39 No. 3, Fall 2008, 411–428

[60] As was awarded in a case of equitable compensation for breach of confidence arising out publication of intimate photographs of his ex-partner by an estranged partner: Wilson v Ferguson [2015] WASC 15 (Supreme Court of Western Australia)

[61] Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era (ALRC Report 123), July 2014, at [6.6] – [6.16]

intentionally or recklessly, and that cannot be justified in the public interest, and also confined to invasions of privacy either by intrusion upon seclusion or by misuse of private information[62].

6.5 How data privacy interests and 'harms to privacy' fit together

A focus upon data privacy interests reflects a 'harms to privacy' approach (as first articulated by Professor Dan Solove[63]). The 'harms to privacy' approach conceptualises privacy by focusing on specific types of disruption to individuals rather than looking for a common denominator that links all of them. In other words, you look for risks of harms to individuals that are occasioned through uses of personal information about them, and characterise data privacy by reference to any collections and uses of personal information that could occasion these risks of harms suffered by the individual and by reference to ability to control such harms.

Data privacy risks and harms go beyond actual or expected monetary, physical, or psychological harm. Many other harms can stem from data privacy risks. [64]

The Intel draft "*Innovative and Ethical Data Use Act of 2019*"[65] provides an excellent illustration of how a data privacy statute might implement a 'privacy harms approach'.

The Intel draft Act does not define "data privacy" at all. Instead, it opens with a proposed legislative statement that "Individuals need to be confident that data that relates to them will not be used to harm them, their families, or society". The draft Act then goes on to note that "the use of personal data by organizations can greatly benefit individuals and society". It proposes a definition of "societal benefit" as a material, objective and identifiable positive effect or advantageous outcome accruing to the public as a result of the processing of

[62] Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era (ALRC Report 123), July 2014, at [1.4]. Compare the American Law Institute's Restatement (Second) of Torts § 652A (1977), pursuant to liability for invasion of privacy would arise where one person intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another (either as to person or private affairs or concerns) and this intrusion would be *highly offensive to a reasonable person of ordinary sensibilities*.

[63] D Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087, 1099

[64] Daniel Solove, A Taxonomy of Privacy,(2006) 154 U.Pa.L Rev. 477; Sean Brooks et al., NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems 10 (Jan. 2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

[65] Available at https://usprivacybill.intel.com/legislation/. The Intel draft Act and its focus upon design and implementation by regulated entities of privacy programs largely reflects the Privacy Risk Management approach in the , which proposes "a cross-organizational set of processes for identifying, assessing, and responding to privacy risks", where "privacy risk" is defined as "the likelihood that individuals will experience problems resulting from data processing, and the impact should they occur". These processes should identify and mitigate "Problematic Data Action", being "data action that could cause an adverse effect for individuals". As with the Intel draft Act, "privacy" is largely used as an adjective and is not defined: NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, January 16, 2020, Version 1.0: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf. In October 2019, the FTC provided positive feedback on a preliminary draft of the NIST Privacy Framework, indicating that it may in the future decide to view this newer publication through a similar lens.

personal data", that is "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".

The Intel draft Act then proposes a definition of "privacy risk" that relate processing of personal data to privacy harms, as listed below. The listed harms largely reflect the taxonomy of privacy harms as initially propounded by Professor Daniel Solove[66] and elaborated and restated in subsequent academic literature.[67] "Privacy risk" means:

> potential adverse consequences to an individual or society arising from the processing of personal data, including, but not limited to:
>
> (A) Direct or indirect financial loss or economic harm;
>
> (B) Physical harm;
>
> (C) Psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma;
>
> (D) Significant inconvenience or expenditure of time;
>
> (E) Negative or harmful outcomes or decisions with respect to an individual's eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or the granting of less favourable terms), housing, education, professional certification, or the provision of health care and related services;
>
> (F) Stigmatization or reputational harm;
>
> (G) Disruption and intrusion from unwanted commercial communications or contacts;
>
> (H) Price discrimination;
>
> (I) Effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relate that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity assessing privacy risk, that significantly—

[66] See in particular Solove, Daniel J, "Conceptualising Privacy", (2002) 90 California Law Review 1087; Solove, Daniel J, Understanding Privacy (2008) and Solove, Daniel J., "A Taxonomy of Privacy", 154 U. Pa. L. Rev. 477, 526–29 (2005)

[67] Calo, M. Ryan, "The Boundaries of Privacy Harm", (2011) Indiana Law Journal Vol. 86 pp1131-1162; Ryan Calo, "A Long-Standing Debate: Reflections on Risk and Anxiety: A Theory of Data Breach Harms by Daniel Solove and Danielle Keats Citron", 96 Tex. L. Rev. Online 59-62 (2018).

(i) alter that individual's experiences;

(ii) limit that individual's choices;

(iii) influence that individual's responses; or

(iv) predetermine results or outcomes for that individual; or

(J) other demonstrable adverse consequences that affect an individual's private life, including private family matters, actions, and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected, observed, or used.[68]

These privacy risks are then proposed to be addressed as follows:

- A regulated entity must implement a "comprehensive privacy program" "designed to: (1) consider and protect an individual's privacy throughout the information life cycle; (2) facilitate an individual's control over personal data, including the ability to participate in decision-making regarding the processing of that personal data; …(5) protect against reasonably foreseeable threats and vulnerabilities to the security of personal data or to the legitimate privacy interests of an individual, …. (6) *identify, assess, and mitigate privacy risk on an ongoing basis*. [69]
- The comprehensive privacy program must include "Ongoing Risk Assessment and Mitigation". The provision is long, but a fair statement of current best practice and accordingly set out in full below:

  "(6) Ongoing Risk Assessment and Mitigation.— A covered entity shall develop, document, and implement an ongoing, entity-wide process to identify, assess, and mitigate reasonably foreseeable privacy risk, including privacy risk raised by new products, services, technologies, methods of processing, and business models. Such process shall do the following:

  (A) Identify reasonably foreseeable internal and external threats that could result in unauthorized access, destruction, acquisition, disclosure, or use of personal data, or of systems containing personal data;

  (B) Assess the likelihood and potential severity of privacy risk created by the processing of personal data, and from unauthorized access, destruction, acquisition, disclosure, or use of personal data, including misuse of personal data by third parties;

[68] Third draft "Innovative and Ethical Data Use Act of 2019", Section 3. Definitions
[69] Third draft "Innovative and Ethical Data Use Act of 2019", sections 2(d) and 4 (Implementation of Fair Information Practice Principles through establishment of a comprehensive privacy program)

(C) Assess the sufficiency of its technical, physical, and administrative controls to identify and mitigate privacy risk and other potential risk from unauthorized access, destruction, acquisition, disclosure, or processing of personal data;

(D) Assess the degree to which technical or operational measures have been taken to de-identify the personal data so as to reduce mitigate the risk of privacy risk to the individual;

(E) Assess the effectiveness of efforts to properly destroy and dispose of personal data, including through the disposal or retirement of hardware or the transition to new software;

(F) Assess the privacy risk from the use of algorithmic, machine learning or artificial intelligence processing of personal data. Such assessment shall include determinations of:

(i) The relevance, accuracy, and adequacy of the data used to train the algorithm or analytical tool;

(ii) The degree to which an individual employed or retained by the covered entity should be involved in the decision making or oversight of the results of the processing covered by this paragraph; and

(iii) Whether it is likely the processing will result in unreasonable privacy risk; and

(G) Assess the potential to reduce or mitigate privacy risk by the deployment of privacy enhancing technologies;

(7) Program Risk Assessment and Validation.— A covered entity shall conduct a periodic assessment, in any event no less than annually, of the privacy program and supporting processes to ensure compliance with this Act. The results of these assessments and any recommendations for changes to the program shall be reported to the appropriate personnel within the covered entity, including senior management."[70]

- Note that the comprehensive privacy program is separate from openness requirements and therefore additional to a requirement to publish a "General Notice"[71] and "Complete Notice" (together akin to an APP1.3 privacy policy) and an Explicit Notice[72] (akin to an APP5.1(a) privacy notice (notice at collection)).
- A comprehensive privacy program must include administrative, technical, and physical privacy protections which are appropriate to the size and complexity of an organization, and the nature and scope of the organization's activities with respect to personal data,

[70] Third draft "Innovative and Ethical Data Use Act of 2019", section 4(h)(Accountability)(6) and (7)
[71] Third draft "Innovative and Ethical Data Use Act of 2019", section 4(f)(Openness)(2)
[72] Third draft "Innovative and Ethical Data Use Act of 2019", section 4(f)(3)

as well as the privacy risk associated with personal data, including its misuse by other organizations that transfer or receive that data.[73] "To be effective, data security and privacy considerations must be part of the day-to-day operations of an organization."[74]

- Additional internal accountability requirements include that an entity must internally publish and implement written policies and procedures implementing the requirements of this Act, conduct training and appoint a data privacy leader responsible for developing and implementing the entity's privacy program and related policies and practices.
- A regulated entity must meet the a "standard for processing", *being a legal obligation when processing personal data of an individual to prevent reasonably foreseeable privacy risk to that individual*.[75] A regulated entity violates the standard for processing if the entity acts with reckless disregard for privacy risk to an individual arising out of the processing of the individual's personal data.
- In determining if a covered entity violated the standard for processing in a given context, factors for consideration are: (a) The covered entity's intent to undertake the processing that caused the privacy risk to the individual (even if the entity did not intend to cause privacy risk; (b) the foreseeability of privacy risk to the individual; (c) the closeness or proximity of the connection between the entity's processing activity and the severity of privacy risk suffered by the individual; and (d) the availability, cost, and commonness of measures that could have been taken to mitigate the privacy risk.[76]

The requirement for a regulated entity to develop and implement a comprehensive privacy program is common to recent draft data privacy statutes built upon an accountability principle.[77] By way of example, the Personal Data Protection Bill, 2019 of India, as introduced into the Lok Sabha, provides:

> 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;

[73] Third draft "Innovative and Ethical Data Use Act of 2019", section 4 (Implementation Of Fair Information Practice Principles Through 9 Establishment Of A Comprehensive Privacy Program)
[74] Third draft "Innovative and Ethical Data Use Act of 2019", section 2(e)
[75] Third draft "Innovative and Ethical Data Use Act of 2019", Section 3. Definitions, para (l) (Standard for Processing). See also CIPL, What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework, May 2020, available through https://www.informationpolicycentre.com/cipl2020amr.html; Lynn Goldstein and other IAF authors, Brenuda Report on Information Accountability, Paper prepared by the Information Accountability Foundation for the Office of the Privacy Commissioner for Bermuda, 28 March 2020, https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/f70f79_199e97af7ae640adbc10cd07eba34470-1.pdf
[76] Third draft "Innovative and Ethical Data Use Act of 2019", Section 3. Definitions, para (l)(1)(a)-(d)
[77] See, for example, Section II – Good Practice and Governance of the Brazilian Privacy Act (Law No. 13, 709 of August 14, 2018)

(b) the obligations of data fiduciaries;

(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.

As a policy construct, the accountability principle focuses on whether a regulated entity has created internal processes that are commensurate with risks and threats. 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. Design and technology choices are not mandated, but the basis for choices should be documented. As noted by Daniel Solove and Paul Schwartz in their commentary on the American Law Institute *Principles of Law, Data Privacy*:

> Any organization can claim that it is practicing privacy by design, but mandated documentation forces organizations to create a record that later can be evaluated and critiqued by regulators or others. This step adds accountability to the process. Documentation showing that the design process for privacy was incomplete or poorly conceived could be damaging later on, as during a post-breach litigation. Our hope is that the documentation requirement will prevent organizations from treating privacy by design as a meaningless shibboleth.[78]

One unusual feature of the Intel draft Act is that it defines the legal obligation ("standard for processing") based upon regulated entity's program of assessment of privacy risk and harms and whether reasonably foreseeable privacy risks to individuals were appropriately managed. It is then a matter of choice for the legislature as to the legal liability principle applied: the Intel draft Act uses "acts with reckless disregard for privacy risk to an individual arising out of the processing of the individual's personal data", but that standard could be

[78] Solove, Daniel J and Schwartz, P.M., "ALI Data Privacy: Overview and Black Letter Text" (January 24, 2020), (2020) UCLA Law Review, Vol. 68, at page 27

defined anywhere on the continuum of well accepted legal concepts of standards of care and negligence.[79]

Although the Intel draft Act uses "privacy", an undefined term, in operative provisions, it is not required to be defined in order to apply the "standard for processing" provisions. In this sense, the Intel draft Act is a 'bottom-up' statute in the 'privacy harms' sense: look for privacy risks to individuals, manage those risks to avoid harms, and if a harm then occurs, consider the management program of the regulated entity both determine whether the provider appropriately assessed and managed risk.

Many other features of the Intel draft Act reflect the mainstream of recent data privacy statutes: broadly, requirements for clearer notices and enhanced consent thresholds, a limited legitimate business interests exception, conventional definition of personal data, provision addressing algorithmic effects, and so on.

The Intel draft Act gives a central role to responsibility and accountability of the regulated entity for assessment of privacy risks and liability for certain harms as occur if those risks are suffered by affected individuals. The approach broadly reflects mainstream thinking of various civil society organisations and forums for data protection regulators discussing enhanced risk and impact assessment and risk management and accountability for regulated entities.[80]

A similar, but more graduated approach is promoted by the Information Accountability Foundation (**IAF**) in the IAF's Model Legislation.[81] This draft Act is built upon two foundational principles, elaborated in a two page introductory section (Section 102, Findings and Purpose)[82] and in outline:

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

Although the term "harm" is not used in the Model Legislation, it follows a similar risk assessment and 'privacy harms' approach to that taken in Intel draft Act. The non-

[79] As to remedies and enforcement for privacy harms, see "Section 14: Enforcement" in Solove, Daniel J and Schwartz, P.M., "ALI Data Privacy: Overview and Black Letter Text" (January 24, 2020), (2020) UCLA Law Review, Vol. 68

[80] See for example the materials referenced in footnote 12 above.

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

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

exhaustive list of examples of "adverse processing impacts" also derives from Daniel Solove's taxonomy of privacy harms[83]. Relevant key concepts are:

- *adverse processing impact*, meaning the detrimental, deleterious, or disadvantageous consequences to an individual arising from the processing of that individual's personal data or to society from the processing of personal data.

  The definition includes a non-exhaustive list of examples as follows:

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

  (2) physical harm,

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

  (4) inconvenience or expenditure of time,

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

  (6) stigmatization or reputational harm,

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

  (8) price discrimination,

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

  (A) alter that individual's experiences,

  (B) limit that individual's choices,

  (C) influence that individual's responses, or

  (D) predetermine results or outcomes for that individual,

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

(10) other detrimental or negative consequences that affect an individual's private life, including private family matters, actions, and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected, observed, or used; and

(11) with respect to detrimental, deleterious, or disadvantageous consequences to society arising from processing personal data, such other demonstrable consequences that may negatively impact a community or the public, taking into account factors such as national security, consumer confidence, the effective and efficient operation of government, effect on the public welfare, or ongoing or disproportionate allocation of risk on a particular population or community.[84]

(Note that (11) addresses societal harms, which are not addressed in the GDPR or in most statements of privacy harms, including the statement on the Intel draft Act. Consideration of societal harms (e.g. loss of social trust) requires difficult judgements concerning the definition, identification and concreteness of such harms. This leads to concern as to whether regulated entities are well placed to assess them. Although consideration of societal harms may be relevant, there would need to be criteria and proxies for such societal harms that are objective and measurable, and evaluation would need to remain grounded in concrete risk to individuals. Given these complexities, this paper does not endorse inclusion of societal harms as a separate privacy harm.)

- *processing risk*, meaning the level of adverse processing impact potentially created as a result of or caused by processing, a specific processing activity, or a specific processing action, assessed as a function of the customary factors, being:

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

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

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

More unusually, the IAF proposes that "processing risk" is assessed applying five distinct levels:

(A) MINIMAL.—Processing that could reasonably be expected to create trivial, negligible, or de minimis adverse processing impact.

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

(B) LOW.—Processing that could reasonably be expected to create minor or limited adverse processing impact

(C) MODERATE.—Processing that could reasonably be expected to create serious or significant adverse processing impact.

(D) HIGH.—Processing that could reasonably be expected to create severe or major adverse processing impact.

(E) EXTREME.—Processing that could reasonably be expected to create dire or catastrophic adverse processing impact.[85]

Article IV (Accountable Processing) proposes a requirement that a covered entity establish and implement an accountable processing management program, addressing the overall direction, management and oversight of processing across the covered entity.

Article V (Processing Risk Management) proposes a requirement that a covered entity establish and implement a risk management program to identify, assess, mitigate and monitor processing risk on an ongoing basis.

To quote the IAF:

> "Section 5.03 provides a limited set of rebuttable presumptions to illustrate how a covered entity should categorize risk in different contexts. Covered entities will be required to make informed decisions, exercise judgment and be accountable for their actions. There are no bright line tests and the assessment of risk in a given context can be challenging."[86]

The multiple categories of risk might appear to create undue complexity, but as they are principally used to set rebuttable presumptions, there is limited jeopardy for regulated entities in misclassification between individual levels.

We noted above that to meet proposed requirements of the Intel draft Act, a regulated entity must meet the a "standard for processing", being a legal obligation when processing personal data of an individual to prevent reasonably foreseeable privacy risk to that individual. Section 2.03 (Unethical And Reckless Processing) in the IAF Model Legislation is analogous to that proposal. Regardless of the legitimate use or permissible basis for processing, when processing the personal data of an individual a regulated entity has a legal duty to that individual to take measures to prevent reasonably foreseeable adverse processing impact to that individual. A regulated entity violates this legal duty *when it acts*

[85] Sept. 23, 2019 draft, at lines 311-329 and 1201-1214

[86] IAF, Summary of "Fair And Open Use Act", January 2020, page 4, available through https://informationaccountability.org/publications/ at https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/Summary-with-logo-for-release-january-2020-1-1.pdf

with reckless disregard for processing risk or for adverse processing impact to the individual.[87]

6.6 RECOMMENDATION 2: APP entities should be required to demonstrate accountability to affected individuals, through introduction into the Privacy Act 1988 of a legislated requirement for APP entities to conduct a comprehensive privacy program and to meet a new legislated standard of care

This paper commends the approach in the Intel draft Act, creating accountability by (1) requiring APP entities to design and implement a comprehensive privacy program to identify, mitigate and manage residual risks of privacy harms to affected individuals arising from collection, use and disclosure of personal information about those affected individuals, and (2) creating a standard of care that is specifically related to listed factors, of which design and implementation of a comprehensive privacy program should be a key factor (with the nature and scope of that program to be determined taking into account the size of the entity and the level of privacy risks associated with collection and handling of personal information by the entity).

The regulatory objective should be to create appropriate regulatory incentive for good data privacy practice by regulated entities. The regulator should be given appropriate direction and enforcement powers, and capabilities, to ensure that these proposed obligations are given effect.

If the regulator is given these powers and capabilities, we do not suggest that a private right if action is conferred upon affected individuals.

6.7 Avoiding the problems with PIAs: the three step action and consequence approach of recent data privacy statutes

The duty of care approach avoids a *three step action and consequence approach* which is inherent in many recent data privacy statutes:

- *What is the legal threshold at which a privacy impact assessment must be done?*

  If this threshold is reached, a regulated entity must undertake a privacy impact assessment that meets prescribed requirements.

[87] Sept. 23, 2019 draft, at lines 555-560. Various factors are listed for assessing whether an entity engaged in processing with reckless disregard in a given context: see lines 561-579. They include intent, the foreseeability of the processing risk or the adverse processing impact to the individual, the closeness or proximity of the connection between the processing and the severity of adverse processing impact suffered by the individual, and the extent to which the measures that could have been taken to mitigate processing risk were reasonably available or considered industry best practice at the time of the processing.

- *What is the threshold at which risks of harms (after implementation of amelioration measures) are determined as legally unacceptable and accordingly a regulated entity should not do an act or undertake a practice?*
- *What is the connection between a privacy impact assessment and a program of processes, controls and safeguards within a regulated entity and the extended data ecosystem (usually also involving other entities) that this regulated entity controls or enables?*

As we will see in section 7 of this paper, statutory drafting to implement the three step action and consequence approach introduces a degree of arbitrariness and therefore uncertainty and liability exposure for regulated entities. It also increases the possibility that some regulated entities may 'game' the requirements for undertaking privacy impact assessment or unfairly shift responsibility for managing some privacy risks to affected individuals.

6.8 Is a 'privacy harms'-based approach *really* that unconventional?

The Australian Law Reform Commission's *For Your Information: Australian Privacy Law and Practice* Report[88] remains the most comprehensive assessment of policy for data privacy regulation in Australia.

In the intervening years there have been substantial advances in policy thinking as to processes for enhanced risk and impact assessment and risk management and accountability for regulated entities. It is these advances that underlie the recommendation as to legal requirements for accountability of APP entities by design and process and an associated duty of care.

That recommendation requires a clear regulatory specification of privacy harms that are required to be assessed, mitigated and managed. In this regard, the ALRC's analysis of *what is privacy* and as to *privacy harms* remains largely current.

After considering various formulations of an individual's right to privacy, the ALRC advocated[89] a combined approach to characterisation of a right of privacy, combining:

- "top-down", "an over-arching conception of privacy, albeit expressed at a high level of abstraction and therefore not free from contention", and
- "pragmatic, bottom-up", identifying harms to individuals occasioned by collection, uses and disclosures of personal information about them.

[88] Australian Law Reform Commission's For Your Information: Australian Privacy Law and Practice (Report 108), May 2008. Volume 1 is available at https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol1.pdf
[89] ALRC, For Your Information: Australian Privacy Law and Practice, at para [1.54] (page 147) and [1.68] (page 150)

This combined approach brought together what the ALRC characterised as "the NZLC's blended 'core values'"[90] and Professor Dan Solove's 'harms to privacy' approach', where:

- "the 'core values' approach recognises 'privacy as a sub-category of two interconnected core values'—namely, the autonomy of humans to live a life of their choosing; and the equal entitlement of humans to respect" ('not to be turned into an object or thing');[91] and
- the 'harms to privacy' approach conceptualises privacy by focusing on the specific types of disruption and the specific practices disrupted, rather than looking for the common denominator that links all of them.[92] In other words, look for harms to individuals that are occasioned through (among other things) uses of personal information about them, and characterise data privacy as a right by reference to the right of an individual to control collection and uses of that personal information that could occasion this harm upon the individual.[93]

6.9 RECOMMENDATION 3: Privacy harms should be identified in the Privacy Act 1988 by a non-exhaustive list

Privacy harms should be identified in the Privacy Act 1988 by an non-exhaustive list and linked to proposed accountability requirement pursuant to which APP entities would be required to design and implement a comprehensive privacy program to identify, mitigate and manage residual risks of privacy harms to affected individuals arising from collection, use and disclosure of personal information.

6.10 RECOMMENDATION 4: Regulatory requirements should reflect good global regulatory practice, but Australia should not be a front-runner

International competitiveness of Australia based businesses should be taken into account in designing regulatory requirements.

The requirements proposed above reflect emerging good regulatory practice.

Australian regulation should reflect good global regulatory practice.

Australia should not be a regulatory frontrunner to the extent that should not substantially disadvantage APP entities as compared to regulation of comparable businesses in other jurisdictions that also implement regulation in accordance with emerging good regulatory practice.

---

[90] New Zealand Law Commission, Privacy Concepts and Issues: Review of the Law of Privacy Stage 1, Study Paper 19 (2008), [2.37].
[91] ALRC, at [1.54]
[92] ALRC, For Your Information: Australian Privacy Law and Practice, at para [1.63] (page 149) citing D Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087, at 1130.
[93] See ALRC at [1.62]-[1.68]

7 The role of privacy impact assessments (PIAs)

7.1 PIAs in the APPs

The OAIC has stated its view that "a privacy impact assessment is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact".[94]

Privacy impact assessments (**PIAs**) have been a recognised feature of data privacy practice for many APP entities for some years.

APP 1.2 requires APP entities to take "such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that will ensure that the entity complies with" the APPs. The OAIC has stated its view of operation of APP1.2 in relation to PIAs as follows:

> In this way, the APPs may be interpreted as requiring 'privacy by design', an approach whereby privacy compliance is designed into projects dealing with personal information right from the start, rather than being bolted on afterwards. Conducting PIAs helps entities to ensure privacy compliance and identify better practice.

However, the status of PIAs under the Privacy Act 1988 has otherwise been somewhat unclear, other than for Australian Government agencies. The *Privacy (Australian Government Agencies – Governance)* APP Code 2017 (the **Code**)[95] commenced on 1 July 2018 and applies to all Australian Government agencies subject to the Privacy Act 1988 (except for Ministers). It is a binding legislative instrument.

The Code sets out specific requirements and key practical steps that agencies must take as part of complying with Australian Privacy Principle (APP) 1.2. This includes a requirement to undertake a written PIA for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information. This is the first time that an instrument under the Privacy Act 1988 has required evaluation of circumstances in which an act or practice affecting data privacy creates high privacy risk.

---

[94] OAIC, Guide to undertaking privacy impact assessments, last revised May 2020, available at https://www.oaic.gov.au/assets/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments.pdf; OAIC, Assessing privacy risks in changed working environments: Privacy Impact Assessments, 6 April 2020, https://www.oaic.gov.au/privacy/guidance-and-advice/assessing-privacy-risks-in-changed-working-environments-privacy-impact-assessments/, further resources at https://www.oaic.gov.au/privacy/guidance-and-advice/assessing-privacy-risks-in-changed-working-environments-privacy-impact-assessments/

[95] https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/australian-government-agencies-privacy-code/

Section 12.2 of the Code states that a project 'may be a high privacy risk project if the agency reasonably considers that the project involves any new or changed ways of handling personal information that *are likely to have a significant impact on the privacy of individuals.*'

The Commissioner may direct an agency to undertake and give a privacy impact assessment to the Commissioner: section 33D of the Act. For the purpose of this provision, a privacy impact assessment is a written assessment of an activity or function that identifies the impact that the activity or function might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact, but without limiting other matters that the PIA may deal with.

Other than where the Code applies, the OAIC "strongly encourages entities to conduct PIAs as a matter of course for projects that involve personal information. Undertaking a threshold assessment — the first step in the PIA process, outlined below — can assist entities to determine whether a PIA is necessary for a project, and should be routinely conducted for every project. The greater the project's complexity and privacy scope, the more likely it is that a comprehensive PIA will be required, to determine and manage its privacy impacts."[96]

In May 2020 the OAIC issued *Draft privacy resource: When do agencies need to conduct a privacy impact assessment?*[97], expressing its main purpose as to help agencies determine when a PIA is required under the Code.

The draft relevantly stated:

> What is a 'significant impact'?
>
> A privacy impact in this context is anything that could adversely affect individuals' information privacy. Impacts include intrusions, such as the collection of new or additional types of personal information, or when the handling of personal information results in an individual losing control over their personal information.
>
> An impact on the privacy of individuals will be 'significant' if the consequences of the impact are considerable, taking into account their nature and severity.
>
> The consequences of a privacy impact could be significant for one individual or a group of individuals, for example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft. The consequences of the potential privacy impacts for a group of individuals may vary

[96] OAIC, Guide to undertaking privacy impact assessments, last revised May 2020, page 4
[97] As available at https://www.oaic.gov.au/engage-with-us/consultations/draft-privacy-resource-when-do-agencies-need-to-conduct-a-privacy-impact-assessment/

based on their individual circumstances, so you should consider whether some individuals may be more significantly impacted than others.

Sometimes projects can have a significant collective impact on society, rather than impacting on people individually. These collective impacts are likely to lead to broad public concern, for example, increased surveillance and monitoring activities, or the establishment of sensitive information sharing arrangements between the Commonwealth and other entities.

There is no definitive threshold to determine when an impact is 'significant' given each project will differ in nature, scope, context and purpose. Accordingly, agencies are advised to screen for factors that may raise a project's risk profile.[98]

The draft also provided a "non-exhaustive list of general and activity-based risk factors which may point to the potential for a high privacy risk project, for use in completing an assessment template. The list was as follows:

- handling large amounts of personal information
- handling sensitive information
- sensitivities of the context in which the project will operate
- handling personal information of individuals who are known to be vulnerable
- handling personal information in a way that could have a serious consequence for an individual or a group of individuals
- activities of a long or permanent duration
- the following activity-based risk factors:
    - ♦ using or disclosing personal information for secondary purposes
    - ♦ disclosing personal information outside your agency
    - ♦ using or disclosing personal information for profiling or behavioural predictions
    - ♦ using personal information for automated decision-making
    - ♦ systematic monitoring or tracking of individuals
    - ♦ collecting personal information without notification to, or consent of, the individual

[98] Ibid., at page 3.

- data matching (linking unconnected personal information)
- developing legislation to modify the operation of one or more APPs or which seeks to rely on the required or authorised by law exception to the APPs.[99]

7.2 PIAs under GDPR

The GDPR is explicitly based on the notion of a risk-based approach.

Recital 74 of the GDPR states that measures of controllers should take into account the risk to the rights and freedoms of natural persons. Various provisions in Chapter IV of the GDPR on the obligations of the controller and the processor specifically refer to "risk", "high risk" and risk assessment (including data protection impact assessment).

The GDPR effectively incorporates a risk-based approach to data protection, requiring organisations to assess the "likelihood and severity of risk" of their personal data processing operations to the fundamental rights and freedoms of individuals. This approach implements what might be referred to as *scalability*: compliance and accountability measures should be appropriate to the nature, scope, context and purposes of the processing.

That noted, a DPIA is only mandated where a type of processing is "*likely to result in a high risk to the rights and freedoms of natural persons*": GDPR Article 35(1).

Article 35(3) provides some examples when a processing operation is "likely to result in high risks":

> (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;[100]
>
> (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10;[101] or

[99] Ibid., at page 4

[100] Summarised in recital 71 as "in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles"

[101] Summarised in recital 75 as "where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures"

(c) a systematic monitoring of a publicly accessible area on a large scale".

The European Data Protection Board endorsed[102] the WP29 *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01*[103], and accordingly those Guidelines remain the definitive regulatory statement for the GDPR as to "risk", "high risk" and risk assessment. The Guidelines:

- restate the above as "possible relevant criteria",
- suggest that "in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out", but "in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA",[104]
- summarise the criteria as follows:

  1. Evaluation or scoring
  2. Automated-decision making with legal or similar significant effect:
  3. Systematic monitoring:
  4. Sensitive data or data of a highly personal nature
  5. Data processed on a large scale
  6. Matching or combining datasets
  7. Data concerning vulnerable data subjects
  8. Innovative use or applying new technological or organisational solutions
  9. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract " (Article 22 and recital 91).

The Guidelines suggest the following as examples of use of these criteria to identify high risk processing requiring conduct of a DPIA:

- A hospital processing its patients' genetic and health data (hospital information system).
- The use of a camera system to monitor driving behaviour on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates

[102] https://edpb.europa.eu/our-work-tools/our-documents/guideline/data-protection-impact-assessments-high-risk-processing_en
[103] Available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
[104] Ibid., at page 11.

- A company systematically monitoring its employees' activities, including the monitoring of the employees' workstation, internet activity, etc.
- The gathering of public social media data for generating profiles.
- An institution creating a national level credit rating or fraud database.
- Storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials.[105]

Thus, the GDPR effectively incorporates a risk-based approach to data protection, requiring organisations to assess the "likelihood and severity of risk" of their personal data processing operations to the fundamental rights and freedoms of individuals.[106]

The Personal Data Protection Bill 2019 of India (as introduced into the Lok Sabha) proposes a more flexible but analogous approach:

> 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.

7.3 The problem with PIAs: the three step action and consequence approach

We noted in section 6.7 off this paper that the duty of care approach (as described in section 6 and underpinning our Recommendation 2 (Accountability through legislation requirement to conduct a comprehensive privacy program and to meet a new legislated standard of care)) avoids a *three step action and consequence approach* which is inherent in many recent data privacy statutes:

We suggest that statutory drafting to implement the three step action and consequence approach introduces a degree of arbitrariness and therefore uncertainty and liability exposure for regulated entities. The three step action and consequence approach also increase the possibility that some regulated entities may 'game' the requirements for undertaking privacy impact assessment or unfairly shift responsibility for managing some privacy risks to affected individuals.

Those conclusions underpin the following recommendations.

---

[105] Ibid., at page 11

[106] See further Center for Information Policy Leadership (CIPL), Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, CIPL GDPR Interpretation and Implementation Project 21 December 2016, available at https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/12/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf

7.4 RECOMMENDATION 5: Privacy impact assessments should be expressly recognised in the Privacy Act 1988

7.5 RECOMMENDATION 6: Having regard to the accountability requirements elsewhere recommended in this paper and the Self-Management Paper, it is *not* recommended that the conduct of privacy impact assessments is specifically mandated, or that the Act specify thresholds for when a privacy impact assessment should be considered (preliminary risk assessment) or conducted (level of risk threshold assessment)

Privacy impact assessments are one tool that APP entities may use as part of an ongoing, comprehensive privacy program.

It is not recommended that the conduct of privacy impact assessments is specifically mandated or that thresholds are created for when a privacy impact assessment should be considered (preliminary risk assessment) or conducted (level of risk threshold assessment).

Given that risk of privacy harms should be substantially mitigated through ongoing good privacy program management, the primary focus should be on the quality, reliability and verifiability of ongoing privacy program management, not the episodic and project specific conduct of privacy impact assessment. Ongoing program management is also more likely to be effective, adaptive and responsive to changing circumstances and evolving uses and applications of data than one-off or episodic impact assessment.

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

Australian Computer Society, Data Sharing Frameworks: Technical White Paper, September 2017

Australian Computer Society, Privacy in Data Sharing: A Guide for Business and Government, November 2018

Australian Computer Society, Privacy Preserving Data Sharing Frameworks: People, Projects, Data and Output, December 2019

Bennett, C.J., "In defence of privacy: The concept and the regime", (2011) Surveillance & Society 8(4) pp 485-496

Brundage, Miles and others, "Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims", April 2020, arXiv:2004.07213 (Cornell University), https://arxiv.org/pdf/2004.07213.pdf

Calo, M. Ryan, "The Boundaries of Privacy Harm", (2011) Indiana Law Journal Vol. 86 pp1131-1162

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

Coglianese, Cary and Nash, Jennifer, 'Compliance Management Systems: Do They Make a Difference?' (May 7, 2020), in Cambridge Handbook of Compliance (D. Daniel Sokol & Benjamin van Rooij eds., Cambridge University Press, forthcoming)

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

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

DeCew, Judith Wagner, In Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Ithaca, NY and London, Cornell University Press, 1997

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

Hartzog, Woodrow, "The Fight to Frame Privacy", 111 Michigan Law Review 1021 (2013)

Keating, P.J., “The Privacy Imperative in the Information Age Free for All”, speech to The Centre for Advanced Journalism at the University of Melbourne on 4 August 2010, available at http://www.keating.org.au/shop/item/the-privacy-imperative-in-the-information-age-free-for-all---4-august-2010

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

Leonard, Peter, “Jobs Half Done: Getting Smart about Smartphones”, Computers and Law, December 2019

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

Leonard, Peter, “Social licence and digital trust in data-driven applications and AI: a problem statement and possible solutions”, available at https://www.business.unsw.edu.au/research-site/Documents/Peter-Leonard-Social-Licence-and-digital-trust-the-problem-statement.pdf

Mackey, Jared M., “Privacy and the Canadian Media: Developing the New Tort of "Intrusion Upon Seclusion" with Charter Values”, (2012) 2:1 UWO J Leg Stud 3

Monti, Andrea and Raymond Wacks, Protecting Personal Information: The Right to Privacy Reconsidered, Hart Publishing, 2019

Moore, Adam, “Defining Privacy”, Journal Of Social Philosophy, Vol. 39 No. 3, Fall 2008, 411–428

Gavison, Ruth, “Privacy and the Limits of Law”, 89 Yale L.J. 421, (1980)

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

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

Parker, Richard B., “A Definition of Privacy”, (1974) 27 Rutgers L. Rev. 275

Prosser, William l., “Privacy”, 48 Cal. L. Rev. 383 (1960)

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

Simitis, Spiros, “Reviewing Privacy in the Information Society”, (1978) University of Pennsylvania Law Review 135, pp 707-746

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

Solove, Daniel J and Schwartz, P.M., “ALI Data Privacy: Overview and Black Letter Text” (January 24, 2020), (2020) UCLA Law Review, Vol. 68

Solove, Daniel J., “A Taxonomy of Privacy”, 154 U. Pa. L. Rev. 477, 526–29 (2005)

Solove, Daniel J. and Danielle Keats Citron, “Risk and Anxiety: A Theory of Data Breach Harms” 96 Texas Law Review 737 (2018)

Solove, Daniel J, Understanding Privacy (2008)

Thierer, Adam, “The Pursuit of Privacy in a World Where Information Control is Failing”, 36 Harvard Journal of Law and Public Policy 409, 414–17 (2013)

Wacks, Raymond, "What has data protection to do with privacy?", (2000) 6(9) Privacy Law and Policy Reporter 143

Wacks, Raymond, “The Poverty of ‘Privacy’” (1980) 96 Law Quarterly Review 73

Warren, Samuel and Louis Brandeis, “The Right to Privacy”, (1890) Harvard Law Review 193

Westin, Alan, Privacy and Freedom, New York: Athenium, 1970