Submission in response to the Privacy Act Review – Issues Paper, October 2020

Australian Government, Attorney-General’s Department

20 November 2020
Covering letter

20 November 2020

Attorney-General's Department
4 National Circuit
BARTON ACT 2600
By email: PrivacyActReview@ag.gov.au

Dear Attorney-General,

RE: Review of the Privacy Act 1988

Thank you for the opportunity to make submissions in relation to the review of the Privacy Act 1988.

Please find our submission attached.

We have no objection to the publication of this submission.

Please do not hesitate to contact me if you would like clarification of any of these comments.

Anna Johnston
Principal | Salinger Privacy
Introduction

Data is the lifeblood of the digital economy, and will increasingly power decision-making in all sectors of the economy.

Robust data protection regulation is necessary to achieve both consumer protection outcomes, and consistency of the playing field for industry. It will therefore be critical to ensure that the Privacy Act remains fit for its purpose of enabling effective regulation of personal information handling, in line with community and business expectations.

Australia deserves a world-class Privacy Act, which draws best practices from around the globe.

The significant trade-off for tightening the regulation of businesses in some areas will be the creation of a window of opportunity for businesses. Alignment with the General Data Protection Regulation (GDPR) in particular will pave the way for an EU ‘adequacy’ decision, which will drive innovation and growth of the digital economy, especially for Australian small businesses seeking to access EU markets.

This submission addresses the following matters, in response to the Privacy Act Review – Issues Paper, October 2020:

- The definition of personal information
- The flexibility of the APPs
- Exemptions from the Privacy Act
- Notice
- Consent
- A fairness framework
- Strengthening the APPs
- Regulating direct marketing and online targeting
- Other permitted purposes
- Inferring sensitive personal information
- Individual rights
- Penalties
- A direct right of action, and
- A statutory tort of serious invasion of privacy.
Scope and Application of the Privacy Act

Definition of personal information

The Issues Paper asks the following questions:

- What approaches should be considered to ensure the Act protects an appropriate range of technical information?
- Should the definition of personal information be updated to expressly include inferred personal information?
- Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?
- Are any other changes required to the Act to provide greater clarity around what information is ‘personal information’?

Through its Digital Platforms Inquiry, the Australian Competition and Consumer Commission (ACCC) found that the current definition of ‘personal information’ suffers from a lack of certainty around its coverage of technical data. The Office of the Australian Information Commissioner (OAIC) also raised the issue of whether inferred data is within scope, while a multiplicity of stakeholders expressed concerns that the Privacy Act – and in particular, the definition of ‘personal information’ - was not keeping up with the realities of the digital economy.¹

Whether or not any particular piece of data meets the definition of ‘personal information’ is a threshold legal issue for the operation of the Privacy Act: the definition of ‘personal information’ determines the boundaries of what is regulated, and what is protected. Understanding the scope of what is meant by ‘personal information’ – and ensuring that that definition remains fit for purpose – is therefore a critical endeavour in privacy jurisprudence.

The challenges posed to the scope and reach of the Privacy Act come from many different directions: new technologies, new interpretations arising from case law, the increasing risks of re-identification, exponential growth in computing power, advances in fields like data analytics and cryptography, the phenomenon of data breaches, the influence of global debates, and new directions in statute law internationally.

We submit that the definition of personal information requires amendment to:

- Clarify that technical data is included
- Clarify that inferred/generated data is included
- Clarify that online identifiers are included, and do not require strict identification of the individual
- Ensure that the identifiability test is not considered in isolation, and
- Bring the definition of 'de-identification' into line with the GDPR and other jurisdictions

**Coverage of technical data and inferred data**

We submit that the definition of ‘personal information’ in the Privacy Act should be amended to change “about” to “which relates to”.

This amendment would partially help to resolve the lack of clarity around coverage of technical data, in line with the ACCC’s recommendations. It would also bring this definitional element closer into alignment with the Consumer Data Right (CDR) scheme and the telecommunications data retention scheme, as well as the GDPR and other international privacy laws.  

We also submit that the definition of ‘personal information’ in the Privacy Act should be amended to include a drafting note or additional definition to further explicate that “relates to” means:

- if the individual is a subject of the information, or
- if the information concerns or links to the individual, or
- if the intent or effect of the information's handling will be to learn, evaluate, treat in a certain way, make a decision about, influence the status or behaviour of, or otherwise have an impact upon, the individual.

This proposal is to avoid judicial determinations which might otherwise interpret the scope of the phrase with the same narrow ‘subject matter’ focus much criticised in the *Telstra* case.  

We also submit that the definition of ‘personal information’ in the Privacy Act should be amended to make the phrase “identified or identifiable individual”. This would replace the current wording of “identified individual, or an individual who is reasonably identifiable”.

---


Removing the concept of ‘reasonably’ identifiable brings the definition into line with the GDPR and multiple other jurisdictions.

We also submit that the definition of ‘personal information’ in the Privacy Act should be amended to add the phrase “whether the information or opinion is provided, collected, created, generated or inferred”. This amendment would make explicit that inferences drawn from data, or new data generated about an individual (such as customer insights which lead to ratings being applied to a customer profile), are within the scope of the definition.

Following the above recommendations would result in a revised definition as follows:

“personal information" means information or an opinion which relates to an identified or identifiable individual:

(a) whether the information or opinion is true or not; and
(b) whether the information or opinion is recorded in a material form or not; and
(c) whether the information or opinion is provided, collected, created, generated or inferred.

Include individuation

Through the current definition of ‘personal information’, the Privacy Act regulates conduct only when a person is identifiable. However privacy harms can also arise from individuation: the ability to disambiguate or ‘single out’ a person in the crowd, such that they can be tracked, profiled, targeted, contacted, or subject to a decision or action which impacts them, even if that individual’s ‘identity’ is not known. This poses a fundamental challenge for current privacy legal frameworks.

From the digital breadcrumbs we leave behind in the form of geolocation data shed from our mobile devices, to the patterns of behaviour we exhibit online as we browse, click, comment, shop, share and ‘like’, we can be tracked. Tracked, traced, monitored, surveilled; then profiled; and finally targeted … all without the party doing the tracking, profiling or targeting needing to know ‘who’ we are.

The digital environment has turned on its head the assumption that identifiability – in the sense of knowing a person’s ‘identity’ - is only vector for privacy harm. Individuation must be anticipated by privacy laws as well.

These contemporary challenges lead us to conclude that the definition of ‘personal information’ in the Privacy Act no longer meets the needs of a privacy legal framework suitable for the digital age. The current definition of ‘personal information’ fails to consider the privacy risks posed by individuation.
Globally, other jurisdictions have more modern definitions, which clearly anticipate device identifiers, online identifiers and location data being used to identify – or at least ‘single out’ - individuals. Some privacy laws are broadening out the notion of ‘identifiability’ (or even abandoning it altogether) as the threshold element of their definition, such as the GDPR, CCPA, and the Nigerian Data Protection Regulation 2019; as well as the 2019 international standard in Privacy Information Management, ISO 27701.4

So as to enable clarity and consistency in the application of privacy law, and to protect against the potential privacy harms enabled by individuation, we submit that the Privacy Act should be amended, to incorporate a definition for the word ‘identifiable’, as follows:

“(i) able to be identified, or (ii) able to be discerned or recognised as an individual distinct from others, regardless of whether their identity can be ascertained or verified”

We further submit that the test for identifiability should be that an individual will be considered “able to be discerned or recognised as an individual distinct from others”:

“if the individual, or a device linked to the individual, could (whether online or offline) be surveilled, tracked or monitored; or located, contacted or targeted; or profiled in order to be subjected to any action, decision or intervention including the provision or withholding of information, content, advertisements or offers; or linked to other data which relates to the individual”.

This additional layer to the test for identifiability aims to ensure that the scope of the regulation does not over-reach into technologies which do not pose risks of privacy harms, such as the use of sessional or load-balancing cookies which are necessary to make a website work, but which do not then continue to track the user.

By more explicitly embedding the concept of individuation within the core definitional element of ‘identifiability’, the Privacy Act can be modernised to reflect the reality of the digital economy, in line with other recent privacy laws such as the GDPR and the California Consumer Privacy Act (CCPA).

Online identifiers

We submit that the definition of personal information should be amended to include a drafting note to the effect that location data, device identifiers and online identifiers (including cookies, IP addresses, MAC addresses, user IDs), are examples (but not the only examples) of data, identifiers or techniques which can render an individual able to be discerned or recognised as an individual distinct from others.

---

Such an amendment would further help to resolve the lack of clarity around coverage of technical data, in line with the ACCC’s recommendations; and would also help to achieve consistency with the GDPR and privacy laws in other jurisdictions featuring more modern statutes, such as South Africa and Nigeria.  

We further submit that there should be included a drafting note (or a new definition in the Act) to the effect that “device” is to be read expansively, and can include a vehicle such as a car, a mobile device such as a mobile phone, a wearable such as a fitness tracker or location monitor, an implantable such as a pacemaker, or a household device such as a smart TV. This amendment would further help to resolve the lack of clarity around coverage of technical data, in line with the ACCC’s recommendations; and would also help to achieve protection against the types of privacy harms made more prevalent in a digital environment. Unlike the CCPA, the definition should not limit the definition with reference to the connectivity of devices. We note that the scope of ‘personal information’ will still be limited by the requirement that the device is somehow linked to an individual, and that the individual is somehow identifiable.

Additional considerations

While the ‘linkability’ element of the definition of personal information is now relatively uncontested, we submit that for clarity’s sake this should be made plain in the statute. We submit that the definition of personal information should be amended to clarify that:

- the test for identifiability is to be conducted with consideration to the information either alone or in combination with other available information, and
- the test for identifiability is not to be conducted with consideration only to whether the individual is identifiable to the entity collecting or holding the personal information, but must anticipate the likelihood of identifiability being achieved by any intended or likely recipients of the data.

De-identification

We submit that the definition of ‘de-identified’ in the Privacy Act should be replaced with a new definition: “anonymous data means data from which no individual is identifiable”.

This wording offers simplicity and clarity, and consistency with the intent of the GDPR. It also makes clear that to fall within the bounds of this definition (and thus have the benefit of no longer needing to protect the data under privacy laws), no individual can be identifiable from the data.

---


The separate definition of ‘identifiable’ (see above) makes it clear that the test is to be considered by looking at the information in the context of possible linkages with other data sources, rather than in isolation.

We do not recommend word-for-word adoption of the GDPR definition, because it contains a notable weakness: by focussing on the ‘data subject’, data meeting the GDPR definition could still potentially reveal information about a third party (e.g. the passenger of a taxi in the taxi trip dataset scenario,7 because only the taxi driver would be the ‘data subject’). Nonetheless using the term ‘anonymous data’, instead of ‘de-identified’ would align the Privacy Act with the GDPR.

This amendment would also achieve greater clarity for regulated entities. A description of how data has been treated in a statistical sense should not be conflated with an assertion about its legal status under the Privacy Act. By using a word which is an adjective (‘anonymous’), instead of a word which can be either an adjective or a verb (‘de-identified’), this problem of conflation between the two meanings should be ameliorated, if not completely resolved.

Indeed with our clients we counsel against using the word ‘de-identified’ at all, instead preferring the descriptor “data to which de-identification techniques have been applied”.

We also suggest the inclusion of a drafting note to the effect that relevant parts of the Privacy Act (namely, the APPs and the data breach notification scheme) therefore do not apply to the handling of ‘anonymous data’. This amendment would achieve greater clarity for regulated entities and consumers/citizens alike, and would align the Privacy Act with the GDPR.

Either the drafting note or the Explanatory Memorandum for the amending Bill could offer further explication, stating that just because de-identification techniques have been applied to data will not necessarily make the data ‘anonymous’ in the legal sense required here. In particular, it should be clarified that pseudonymous data is not anonymous data; see Article 4 and Recital 26 of the GDPR.

Flexibility of the APPs

The Issues Paper asks the following question:

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

---

In our view the framework of the Act does not appropriately regulate all the entities, acts and practices it should.

While the following section of the Issues Paper focuses on some specific exemptions, it does not include consideration of the exemption at s.7B(5), which in our view creates a significant gap in effective regulation.

When private sector organisations are operating as a contracted service provider under a State contract, the practices involved in fulfilling that contract are exempt from the Privacy Act; see s.7B(5). However this does not necessarily mean that they are bound by a State law equivalent to the Privacy Act. They may be entirely unregulated for those practices.

Nor can private sector contracted service providers ‘opt back in’ to the APPs even if they wanted to; the ‘opt in to the APPs’ method is only available for small businesses (s.6E), and the ‘be prescribed in’ method is only available for State and Territory instrumentalities (s.6F). Even if they agree to be bound by contract to meet a set of standards set by their client through the relevant set of State or Territory privacy principles, that contract is only enforceable by their client, providing no recourse or remedy for individuals who seek to complain about non-compliance with the standards set via that contract, and no investigative powers are triggered for the OAIC or any State or Territory privacy regulator.

By way of example, a large consulting firm which assists public sector clients with data analytics capabilities would typically be bound by the APPs in the Privacy Act because their turnover is more than $3M pa. However to the extent that their clients are State or Territory public sector agencies, which includes public universities, they will not be bound by the APPs. Whether or not they are bound by a State or Territory privacy law instead will differ from State to State (noting SA and WA have no law to bind them to), as well as from client to client, and even from contract to contract.

The same scenario applies to contractors, suppliers and vendors of all manner of goods and services to public sector agencies across State/Territory and local government, as well as public universities.

We have certainly seen private sector suppliers use their market power to refuse to be bound by contract to follow State privacy law when supplying to State government agencies. Yet s.7B(5) means they will be exempt from the APPs, in relation to the personal information they handle as part of their supply of services to the State government.

The effect of s.7B(5) is that a private sector organisation may only sometimes be bound by the APPs in the Privacy Act, sometimes by State or Territory privacy principles (either directly or via contract), and sometimes by no privacy law at all.

We also note that non-profit organisations, in particular in the human services sector (e.g. aged care, disability care and child services) often operate under a mix of regimes. For example a provider of out-of-home-care services for children might receive a mix of funding from different State and Territory governments, each with their own rules: some set as a
condition of their funding, some included in binding contracts, some directly regulated by the State law as a contracted service provider. Yet for areas not directly involved in delivering those client-facing services (e.g. marketing, office administration etc) they will be regulated by the federal Privacy Act. This overlapping patchwork-but-with-gaps approach to privacy regulation poses an immense compliance burden on non-profit organisations - which are arguably the worst-positioned type of organisation to manage such a burden –yet offers no commensurate improvement in private protections for individuals.

We submit that s.7B(5) ought to be amended, such that the carve-out for contracted service providers to State or Territory authorities ought only apply if the organisation is bound directly by a State or Territory privacy law to comply with that State or Territory privacy law as if it were a public sector agency of that State or Territory, such that an individual complainant has a legal mechanism by which they can enforce compliance with the State or Territory privacy law by the contracted service provider, and seek a remedy for any harm suffered.

Alternatively, s.7B(5) ought to be deleted, so that the federal Privacy Act effectively ‘covers the field’ for private sector organisations, even in circumstances where organisations are operating under a State contract and/or receive funding from State or Territory governments. This amendment would however require some co-operation from State or Territory governments to reduce the burden on non-profits in particular from having to comply with both federal and State/Territory requirements.

Exemptions from the Privacy Act

Small business exemption

The Issues Paper asks the following questions:

- Does the small business exemption in its current form strike the right balance between protecting the privacy rights of individuals and avoid imposing unnecessary compliance costs on small business?
- Would there be benefits to small business if they were required to comply with some or all of the APPs?

In our view, the reasons posed in the past to exempt small businesses are no longer valid. In an online world, even small businesses can handle vast amounts of personal information, and can therefore do privacy harm at a scale not imaginable twenty years ago.

Further, as the Issues Paper notes, no other comparable jurisdiction exempts small businesses from its privacy laws. The regulatory burden has not proven too great in other countries.
In fact amongst our client base we have had a number of small Australian businesses which have found themselves regulated by the GDPR, and will shortly be regulated by the New Zealand Privacy Act as well because they offer good or services to overseas customers – yet they do not have to comply with the Privacy Act in their home country. They are already facing – and managing well – their obligations under foreign privacy laws. Inclusion of small businesses within the ambit of the Australian Privacy Act will not be a stretch for those businesses.

In fact small businesses would stand to benefit if the abolition of the exemption helped lead to an ‘adequacy’ decision for Australia from the European Commission, and similar from New Zealand, as cross-border data flows will become straight-forward by comparison to now. This will open up new markets to Australian businesses.

We submit that the small business exemption should be abolished.

We also submit that the OAIC should be significantly better funded to help proactively assist small businesses understand their obligations, as well as to respond to any increase in privacy complaints.

**Employee records exemption**

The Issues Paper asks the following questions:

- Is the personal information of employees adequately protected by the current scope of the employee records exemption?
- If enhanced protections are required, how should concerns about employees’ ability to freely consent to employers’ collection of their personal information be addressed?
- Should some but not all of the APPs apply to employee records, or certain types of employee records?

We submit that the employee records exemption should be abolished.

We suggest that public sector and private sector employees ought to be treated alike, in terms of the base level statutory protection of privacy rights. We also note that since the Privacy Act was extended to the private sector in 2000, the mandatory notifiable data breach scheme has been introduced, which imposes reporting obligations on private sector employers in relation to some aspects of employee records, most notably Tax File Numbers. Employers are thus already obliged to manage the data security of Tax File Numbers. We submit that there is no valid reason to offer less protection to the remainder of employee records.

Taken as a sector overall, we submit that the private sector will benefit from the abolition of the employee records exemption, if it helps lead to an ‘adequacy’ decision for Australia from the European Commission, and similar from New Zealand, as cross-border data flows will
become straight-forward by comparison to now. This will open up new markets to Australian businesses.

Our experience interpreting and annotating NSW privacy case law also serves as a warning against even well-intentioned exemptions for some aspects of employee records. The ‘suitability for employment’ exemption in NSW has been the subject of numerous decisions since 2001. In our view, the only privacy principles which could possibly require an exemption in relation to employment matters are the Access and Correction principles. Most employment scenarios such as where matters are subject to negotiation or possible/actual legal proceedings would already be covered by the exceptions at APP 12.3, but potentially an additional exception to access and correction rights could relate to reference checks at the time of recruitment.

Other obligations, such as the need to ensure only relevant and non-intrusive personal information is collected, that personal information is securely stored, and that the accuracy of personal information is checked prior to making a decision, should all apply in employment scenarios just as they would when dealing with customers’ personal information.

**Political exemption**

The Issues Paper asks the following questions:

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

We submit that the political exemption should be abolished.

Australians need a Privacy Act which is fit for the purpose of protecting our privacy in the digital age. Since this exemption was crafted twenty years ago, we have seen an explosion in the practice of profiling and targeting individuals for bespoke political messaging. Personalised news feeds, ads and other personalised content online can more easily facilitate misinformation than offline political advertising could achieve. As a result, the risks posed – not only to the privacy of individuals but to the public good, including the stability of our democratic government and public trust in public institutions – have exponentially increased since 2000.

There is no sound reason why political parties should not have to be accountable for their management of personal information about constituents and voters, as is already the case in other jurisdictions. An obligation to be transparent about collection practices should apply to political parties, along with obligations to not collect sensitive personal information.

---


9 Section 4(3)(j) of the Privacy and Personal Information Protection Act 1998 (NSW) and s.5(3)(m) of the Health Records and Information Privacy Act 2002 (NSW).

or other intrusive personal information about individuals, as well as obligations to store data securely and not misuse it or disclose it without authority.

Journalism exemption

The Issues Paper asks the following questions:

- Does the journalism exemption appropriately balance freedom of the media to report on matters of public interest with individuals’ interests in protecting their privacy?
- Should the scope of organisations covered by the journalism exemption be altered?
- Should any acts and practices of media organisations be covered by the operation of some or all of the APPs?

The Issues Paper notes a high volume of privacy complaints made about media organisations each year, but under schemes which offer no enforceable resource to remedies for the victims. Examples of gross violations of individuals’ privacy by Australian media organisations which served no public interest journalism purpose have included outing Ashley Madison users on the air for entertainment value;\(^{11}\) and using a helicopter to film a family on their private property, grieving over a dead child.\(^{12}\)

We submit that the journalism exemption should be abolished, and replaced with a limited exemption to the collection, use and disclosure principles (APPs 3, 5 and 6) for activities necessary to the conduct of investigative and public interest journalism.

We submit that existing member-based media industry complaints-handling bodies such as the Australian Press Council could be recognised under s.35A of the Privacy Act as offering an external dispute resolution scheme for investigating and conciliating complaints about breaches of the APPs, so long as effective appeal rights are also established so that complainants can seek enforceable remedies.

\(^{11}\) See https://www.theguardian.com/technology/2015/aug/20/radio-hosts-tell-woman-live-on-air-her-husband-had-ashley-madison-account
\(^{12}\) See https://www.abc.net.au/mediawatch/episodes/private-tragedy-vs-public-interest/9973980
Protections

Notice of collection of personal information

The Issues Paper asks the following questions:

- Does notice help people to understand and manage their personal information?
- Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?

While transparency is important, we submit that this review should not overestimate the effectiveness of notice as a mechanism for delivering meaningful privacy protective outcomes for individuals.

Rather than posing notice (and/or consent) as the primary means by which individuals can ‘manage’ their personal information, a preferable model of privacy regulation is to avoid burdening individuals with having to worry about, or make choices about, their privacy at all.

The problems with notice

The first problem with notice is how it is often implemented in practice, which is to bury consumers in fine print, knowing that almost nobody will bother reading the notice. Rather like the Londoners who ‘consented’ to give up their first born child when signing up for free Wi-Fi, most people don’t read T&Cs, because they are longer than Shakespearean plays.

Notice just doesn’t scale. Artists and consumer groups have sought to illustrate the problem, such as in the video in which the advocacy group Norwegian Consumer Council asks their Consumer Affairs Minister to go for a jog while they read her the privacy policy from her fitness tracker. The Minister manages to run 11km in the time it takes for the policy to be read out to her. When the same group tallied up the T&Cs for the apps found on an ‘average’ mobile phone, reading them took 37 hours. That’s before we grapple with the quagmire posed by the Internet of Things: where on a smart toothbrush is a company going to locate a privacy notice, let alone consumer controls?

Even if a customer does read the fine print, they probably don’t understand that phrases like ‘share data with our partners to personalise your experience’ means the kind of privacy-

---

14 See http://conversation.which.co.uk/technology/length-of-website-terms-and-conditions/
15 See https://flowingdata.com/2018/05/08/comparison-of-terms-and-conditions-lengths/
16 See https://www.youtube.com/watch?v=lgAhTVxlyE
17 See https://www.forbrukerradet.no/side/the-consumer-council-and-friends-read-app-terms-for-32-hours/
invasive profiling practices on which third party data brokers and AdTech thrive. Speaking at a webinar to mark Privacy Awareness Week in May 2020, Privacy Commissioner Angelene Falk noted that the OAIC’s 2020 Community Attitudes to Privacy Survey found that only 20% of people felt confident that they understood privacy policies. Often that is deliberately so.\textsuperscript{18} The Notice of Filing in the OAIC’s lawsuit against Facebook for disclosing the personal information of 311,127 Australian Facebook users in the Cambridge Analytica scandal states: “The opacity of Facebook’s settings and policies hampered (Australian Facebook users) in understanding that their data was disclosed to the app. The design of the Facebook website was such that Users were unable to exercise consent or control over how their personal information was disclosed”.\textsuperscript{19}

Making transparency meaningful

Our submission is that if consumers are looking at a privacy notice at all, they just want to know (quickly, at the point in time that suits them, in language they understand, in a format that works for them) what they would not already expect, what their choices are, and what they don’t have choice about. In other words: \textit{Just tell me now if it is safe for me to proceed}. Or: \textit{Just tell me if this app is safer than this other one}. However because how one person might be harmed is different to the next person, and what one person values is different to what the next person values, and because children are different to adults, that information should be contextual for each person.

European think-tank DataEthics suggests taking a layered approach, and using icons to categorise types of information. They were part of a consultation group reviewing IKEA’s new app, which integrates explanations, toggle controls, prompts and links to more information within the user experience. IKEA’s customer data promise and the app’s design were seen as innovative enough to be the subject of a presentation at the World Economic Forum in Davos early in 2020.\textsuperscript{20}

However user-centric design is not enough. First, we need universal terms and icons, as well as ways to present them better, to quickly communicate privacy messages and choices to individuals of all ages, backgrounds and levels of literacy.

To help consumers better understand data practices and exercise choice, the OAIC has expressed the need for “economy-wide enforceable rules, standards, binding guidance or a code”, to create “a common language in relation to privacy and personal information, which could include the use of standardised icons or phrases”.\textsuperscript{21} The new Consumer Data Right scheme provides a positive example of what can be achieved. The CSIRO’s Data61 has legislated power to set standards under the CDR scheme; their guidance on translating the legal elements of consent into design specifications is extremely valuable.\textsuperscript{22} We note that

\textsuperscript{20} See https://dataethics.eu/designing-for-informed-consent-online-that-works/
under the CCPA, the Californian Attorney General (who for now fulfils the role of the privacy regulator) has the power to make regulations including developing logos and opt-out icons.

Other ideas for improving privacy notices are modelled on successful designs used in safety messaging (traffic light indicators), and product labelling (star ratings, nutrition labels).

Privacy advocate Alexander Hanff has developed a proof of concept matrix of data types, internal uses and disclosure types, each one coloured red, amber or green, allowing users to click through for more information.23

In 2009, researchers in privacy and trust from Carnegie Mellon University and Microsoft presented an idea for using nutrition labelling as a model for communicating privacy messages. Having tested and rejected matrix designs as too complex, their simplified label broke messaging into What, How and Who: what categories of personal information are being collected; the different purposes for which the data will be used, including whether the user can restrict those purposes by opting in or out; and to whom it will be disclosed, including any choice over such disclosures. They struck difficulties: even University students didn’t understand the symbols used to illustrate opting in versus opting out.24

The idea of nutrition labels received a more recent boost from Ghostery President Jeremy Tillman, who argued that the US government should develop uniform labelling: “What consumers need is a privacy nutrition label – something quick and scannable they can look at to see what the privacy impact of a digital service is before they use it, the same way they would look at nutrition info before eating a candy bar”.25

However we argue that this metaphor precisely illustrates the problem: in this scenario, the consumer checks the nutrition label but then still eats the candy bar. If consumers made only rational decisions, they would put down the candy bar and pick up a piece of fruit instead. However that’s not how humans necessarily behave. Sometimes we crave instant gratification, whether that is a sugar rush or to download a game of Candy Crush.

Not waiting for legislative development or international standards, Apple announced recently that it has developed its own privacy ‘nutrition label’, to be applied to all apps offered to users via the Apple App Store from 2021. The labels will list what information an app collects, and present that visually – within the design parameters set by Apple - on the app page.

However nutrition labels still depend on we humans to stop and read them, over and over and over again, and use them to compare one product to another. So this form of notice still doesn’t work at scale.

---

23 See https://www.youtube.com/watch?v=IVuj5qzJiUh&trk=
24 See https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf
25 See https://www.techradar.com/news/the-case-for-a-privacy-nutrition-label
The most innovative idea we have seen in this space comes from Data61, who have proposed a machine-readable solution. Senior experimental scientists Alexander Krumpholz and Raj Gaire wrote: “Wouldn’t it be nice if we could specify our general privacy preferences in our devices, have them check privacy policies when we sign up for apps, and warn us if the agreements overstep?”26

Basing their idea on Creative Commons icons which are universally agreed, legally binding, clear and machine-readable, their proposal would also need legally binding standards and universal icons, but it would work more efficiently than star ratings, traffic light matrices or nutrition labels alone. They propose ‘Privacy Commons’ classifications to cover what they call Collection, Protection and Spread: the categories of personal information collected, the data security techniques applied, and who the personal information will be disclosed to. In our view they need to add also include the purposes for which the personal information will be used within the organisation, but the idea is a great start.

This model would be a significant time-saver, by getting consumers to think deeply once about what they are trying to achieve in terms of their personal privacy goals, and then automating the legwork of reading and comparing privacy policies against those goals.

We submit that the Privacy Act should enable a legal and technology framework which allows an individual to set their own privacy risk profile (e.g. add me to a mailing list is OK, never share my home address, don’t collect my date of birth, don’t collect location data without checking with me, etc), and then facilitates an automated ‘reading’ of a company’s data practices against their profile (and even better, automating the toggling on or off of settings to match their profile), to come up with tailored gatekeeping advice about whether it is safe for them to proceed.

We submit that this model is the best we have seen to date which might actually deliver on the promise of transparency, and its further refinement ought be encouraged by the Australian Government.

Consent to collection, use and disclosure

The Issues Paper asks the following questions:

- Is consent an effective way for people to manage their personal information?
- What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?
- Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?

---

We submit that the definition of consent should be defined narrowly in the Privacy Act, to enshrine the guidance from the Privacy Commissioner that, in order to be valid as a means by which to authorise the collection, use or disclosure of personal information which would not otherwise be allowed, consent must be a clear affirmative act of agreement that is freely given, specific, unambiguous and informed, current and given by a person with capacity.

In particular, consent must be defined in statute such that:

- To be valid, the consent must include the individual's demonstrable, unambiguous, pro-active expression of their wishes; i.e. their choice can only be expressed as ‘opt-in’ (not: opt-out, default or pre-selected settings, silence, or inactivity); and
- To be valid, the consent cannot be ‘bundled’ with other requests for consent, or with terms and conditions over which the user has no choice; and
- To be valid, the consent must be informed, meaning that sufficient information was provided at a degree of comprehensibility suitable for that audience; and the consent was indeed provided by a person with the capacity to comprehend that information; and
- To be valid, the consent must be specific, meaning that the information provided was specific as to the purposes for which the personal information will be collected, used or disclosed (or will not be, unless the individual provides their consent); and
- To be valid, the consent must result in non-discrimination and no penalty (such as unequal service or prices) for the individual.²⁷

However we also submit that for the most part, consent is not an effective way for people to manage their personal information. Consent should not be necessary for the use or disclosure of personal information which is in pursuit of the primary purpose for which the information was collected in the first place, or for directly related secondary purposes.

Consent should be the last option, rather than the first ‘go to’ mechanism for organisations seeking authority to collect, use or disclose personal information.

We submit that the objective of the Privacy Act should be to restrict data flows (i.e. the collection, storage, use and disclosure of personal information) unless they can be justified within a framework of overarching principles including necessity, proportionality and fairness. (See also further discussion below of a fairness framework.)

Stepping outside that framework should be allowed only in exceptional circumstances, in which case the standard set for obtaining consent should be very high.

Consent should be difficult to obtain, for the reasons following.

²⁷ By way of example, the CCPA prohibits unequal service or prices for people who exercise their rights to opt-out of data sale.
It is difficult to get truly informed and voluntary consent

Consumers don’t have enough power, knowledge or time to genuinely exercise what little choice or control they might be offered. There is a power imbalance between consumers and corporations; and between citizens and governments. The OAIC’s submission to the ACCC’s Digital Platforms Inquiry calls this out clearly:

“consumers may be informed and understand the inherent privacy risks of providing their personal information, but may feel resigned to consenting to the use of their information in order to access online services, as they do not consider there is any alternative. Further, while ‘consent’ is only a meaningful and effective privacy self-management tool where the individual actually has a choice and can exercise control over their personal information, studies also show that consumers rarely understand and negotiate terms of use in an online environment”.28

Describing consent as a “legal fiction”, the editorial board of the New York Times nailed the pointlessness of even reading privacy policies: “Why would anyone read the terms of service when they don’t feel as though they have a choice in the first place? It’s not as though a user can call up Mark Zuckerberg and negotiate his or her own privacy policy. The ‘I agree’ button should have long ago been renamed ‘Meh, whatever’.”29

Further, there is an element of elitism and privilege behind the very notion of notice and consent: suggesting to consumers that if they don’t like what’s happening with their privacy, they should just opt out of using Google / Facebook / Uber / etc ignores the reality that much of our civil and political life depends on or is mediated through a small number of dominant technology platforms and service providers.

We also submit that it is a fantasy to think that consumers can calculate the privacy risks arising from every single transaction they enter into, let alone whether the benefits to be obtained now will outweigh the risks to be faced later. Rachel Dixon, the Privacy and Data Protection Deputy Commissioner in Victoria, has said about the role of consent that because most data is collected during transactions where we as consumers or citizens want something, the ‘consent’ obtained is almost never fair: “There is always an inherent lack of attention paid to the downstream consequences”.30

Privacy risks are usually time-shifted, and obscure. In the context of artificial intelligence in particular, ‘consent’ can almost never be informed, because the outcomes of machine learning are not yet known.

If an individual doesn’t understand the risks, their consent will not meet the test for ‘informed’, let alone any of the other elements needed to gain a valid consent.

29 See https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html
30 See https://www.abc.net.au/radio/programs/bigideas/can-computers-make-fair-and-ethical-decisions/11159904
Why we can’t always be informed about privacy risks

One of the reasons companies and governments don’t do a better job of explaining privacy risks to citizens and consumers is because sometimes they don’t even know.

Lawyer Andrew Burt has written about how the nature of privacy risks has shifted. Where once organisations and individuals alike worried about personal information being misused or disclosed without authority, now, in this world of Big Data and machine learning, he suggests the biggest threat comes from the unintended inferences drawn from our personal information: “Once described by Supreme Court Justice Louis Brandeis as ‘the right to be let alone’, privacy is now best described as the ability to control data we cannot stop generating, giving rise to inferences we can’t predict.”

Privacy academic Daniel Solove says it is “nearly impossible for people to understand the full implications of providing certain pieces of data to certain entities. … Even privacy experts will not be able to predict everything that could be revealed… because data analytics often reveal insights from data that are surprising to everyone”. The benefits of ‘consenting’ are usually obvious and immediate, while the possible privacy risks are unpredictable, obscure and time-delayed.

By way of example, the public release of Strava fitness data, although ‘de-identified’, gave rise to privacy and security risks that the company themselves had failed to predict. Strava is a social network of people who use wearable devices to track their movements, heart-rate, calories burned etc, and then share and compare that data with fellow fitness fanatics. After releasing a data visualisation ‘heat map’ of one billion ‘activities’ by people using its app, an Australian university student pointed out on Twitter that the heat maps could be used to locate sensitive military sites.

So if service providers cannot imagine the risks posed by the data they hold, how is a consumer expected to figure it out?

When data is combined from different sources, or taken out of context, or when information is inferred about individuals from their digital exhaust, the privacy issues move well beyond whether or not this particular app, or device, or type of data, poses a risk to the individual. We have to assess the cumulative impact. The herculean task of assessing the likely risks posed to an individual’s privacy means that notice about likely risks is impossible to deliver, and therefore informed consent is impossible to obtain.

31 See https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies
33 See https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de
34 See https://twitter.com/Nrg8000/status/957318498102865920
It’s just not fair

Even if you could magically solve the problems of digital literacy, power imbalances, and the difficulties of calculating privacy risks, and deliver your consent solution at scale, the notice and consent model still suffers a terrible weakness: it’s just not fair.

At the IAPP ANZ Summit in 2019, Law Professor Woodrow Hartzog described how notice and consent, as well as the related idea of solving privacy problems by offering more user controls, are both ways of shifting risks onto individual consumers and citizens. He has also written about the “fallacy” that it is up to us as individuals “to police Facebook and the rest of the industry”.

Even in the context of discussing privacy laws such as the Australian Privacy Act which do not rely entirely on consent – i.e. the consent of the subject is what you need when you can’t rely on any other ground to lawfully collect, use or disclose personal information – Australasian privacy regulators are calling time on the over-reliance of consent as a mechanism, on the grounds of fairness.

NZ Privacy Commissioner John Edwards has said of consent that it asks too much of a consumer, and described it at the same 2019 conference as an “abdication of responsibility”. He has published guidance telling companies to lift their game when it comes to designing consent mechanisms, saying the practice of ‘click to consent’ is simply not good enough anymore.

Likewise, the Australian Privacy Commissioner, in the OAIC’s submission to the ACCC in response to its Customer Loyalty review, has said that “Overreliance on consent shifts the burden to individuals to critically analyse and decide whether they should disclose their personal information in return for a service or benefit.” In a similar vein, the OAIC has also said that that burden “should not fall only on individuals, but must be supported by appropriate accountability obligations for entities, as well as other regulatory checks and balances.”

Consent should be the last resort, not the first or only choice from a menu of regulatory or design responses to privacy problems. The responsibility for protecting our privacy should fall on privacy regulators, government legislators, and organisations themselves – not on individual consumers or citizens.

35 See https://onezero.medium.com/user-agreements-are-betraying-you-19db7135441f
36 See https://privacy.org.nz/blog/click-to-consent-not-good-enough-anymore/
The need for a fairness framework

The Issues Paper asks the following questions:

- Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?
- Should there be some acts or practices that are prohibited regardless of consent?
- Should reforms be considered to restrict uses and disclosures of personal information? If so, how should any reforms be balanced to ensure that they do not have an undue impact on the legitimate uses of personal information by entities?

Even with innovative approaches like machine-readable privacy policies, it is difficult to code for whether any given collection or use of data is necessary, proportionate, reasonable or fair. As privacy and technology lawyer Peter Leonard argues, consumers shouldn’t even be put in the position of having to figure out for themselves whether a company’s data practices are reasonable: “Regulators don’t require consumers to take responsibility for determining whether a consumer product is fit for purpose and safe… Why should data-driven services be any different?”

Successful privacy protection should not depend on the actions of the individual citizen or consumer. Placing the burden of privacy protection onto the individual is unfair and absurd. It is the organisations which hold personal information – governments and corporations – which must bear responsibility for doing no harm.

Thus we need a more wholistic and protective approach to privacy regulation, in which an organisation can only collect, use or disclose personal information when it is fair to do so.

There are some practices so privacy invasive or socially damaging that even ‘consent’ should not be allowed to authorise them. The late Giovanni Buttarelli, European Data Protection Supervisor, argued that “The right to human dignity demands limits to the degree to which an individual can be scanned, monitored and monetised — irrespective of any claims to putative ‘consent’.”

Because we care about human dignity and autonomy, in Australia we do not allow trade in human organs or tissue. ‘Consent’ doesn’t even come into it. It is our submission that it is time we better regulated some forms of data exploitation too.

We submit that the Privacy Act should be reformed to introduce an overarching fairness test, in which even ‘consent’ would not be sufficient to authorise certain data practices. While the Issues Paper only asks about use and disclosure, to adequately regulate practices which commence with data collection, we suggest that all those privacy principles

---

40 See https://iapp.org/media/pdf/resource_center/giovanni_manifesto.pdf
which touch on collection, use and disclosure should be subject to an overarching fairness requirement.

Further, we suggest that simply requiring ‘lawful and fair’ conduct is not sufficient. The requirement should be that all collection, use or disclosure of personal information must be:

- fair (in intent) and reasonable
- lawful
- transparent
- necessary and proportionate
- not unnecessarily intrusive (in either the means of collection or the nature of the data collected), and
- not lead to outcomes which would be unfair or discriminatory, or which would diminish human dignity.

Such a framework could enable more robust review of practices such as marketing to children or other vulnerable populations, the commercial application of facial recognition technology, racial profiling, or algorithms which lead to discriminatory outcomes. The OAIC has proposed introducing a similar “general fairness requirement for the use and disclosure of personal information” as a way of addressing “the overarching issue of power imbalances between entities and consumers” and “protecting the privacy of vulnerable Australians including children”.41

We submit that as part of adopting an overarching fairness framework as outlined above, the OAIC could issue guidance on what would not meet the requirements of that framework.

By way of example, Canadian privacy law includes a gatekeeper provision. Section 5(3) of PIPEDA says: “An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.” As a result the Canadian Privacy Commissioner publishes guidance on ‘no-go zones’, based on court interpretations of s.5(3) as well as consultations with stakeholders and focus groups.42 Of course what is ‘reasonable’, ‘appropriate’ or ‘fair’ are subjective assessments, but the Canadian model at least creates a space for reflecting community expectations in the application of legal tests.

One such area should relate to the tracking, monitoring, profiling or targeting of children. In its report on customer loyalty schemes, the ACCC noted that multiple submissions requested that children should not be tracked, profiled, subject to marketing or monetised.

42 See https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/qd_53_201808/
A second area which should be a ‘no-go’ zone is the tracking and sharing of mental health information other than by the individual’s own health service providers.43

A third area which should be a ‘no-go’ zone is the collection, use or disclosure of precise geolocation data without explicit consent.

One of the key findings of the OAIC’s latest Australian Community Attitudes to Privacy Survey is that 62% of Australians are uncomfortable with their location being tracked through their mobile or web browser.44 This is not unusual: a survey by the New Zealand Privacy Commissioner in 2016 also asked what people found most ‘sensitive’, and 63% responded that they were sensitive about physical location.45 Indeed across continents and cultures the message is the same: sharing location data makes the majority of people feel “stressed, nervous or vulnerable, triggering fears of burglaries, spying, stalkers and digital or physical harm”.46

Yet website and app developers routinely collect location data, quite contrary to community expectations. A global ‘sweep’ of more than 1,200 mobile apps by Privacy Commissioners around the world in 2014 found that three-quarters of all the apps examined requested one or more permissions; the most common was location.47 Disturbingly, 31% of apps requested information not relevant to the app’s stated functionality. A prominent example was a torch app which tracked users’ precise location, and sold that data to advertisers.48 More recently, a scan of 136 Covid-19-related apps for the Defcon security conference found that three quarters asked for location data, even in apps where the stated functionality was simply to monitor the user’s symptoms.49

Location data is highly granular. One study suggested that four points of geolocation data alone can potentially uniquely identify 95% of the population.50 Mark Pesce, a futurist, inventor and educator, has described the geolocation data collected by and broadcast from our smartphones as “almost as unique as fingerprints”.51

Data showing where a person has been can reveal not only the obvious, like where they live and work or who they visit, but it may also reveal particularly sensitive information – such as

---

43 See the report of an investigation by Privacy International at https://privacyinternational.org/long-read/3194/privacy-international-investigation-your-mental-health-sale
46 See https://dataethics.eu/sharing-location-data-makes-consumers-uneasy/
51 Mark Pesce was keynote speaker at the OAIC Business Breakfast for Privacy Awareness Week in May 2015; this quote is from the author’s contemporaneous notes from the event.
if they have spent time at a church or a needle exchange, a strip club or an abortion clinic. Some app-makers claim they can even tell which floor of a building people are on.\textsuperscript{52}

A recent example is the analysis conducted by Singaporean company Near on the movements of workers at an abattoir in Melbourne, which was the centre of an outbreak during the first COVID-19 isolation period.\textsuperscript{53} Near claimed that it could track this small cohort of workers to specific locations including shops, restaurants and government offices. (Near uses “anonymous mobile location information” collected “by tapping data collected by apps” to provide insight into the precise movements of individuals, in order to offer advertisers “finer slices of audiences to reach highly qualified prospective customers”.\textsuperscript{54} Near boasts of having “the world’s largest data set of people’s behavior in the real-world” consisting of 1.6 billion ‘users’, across 44 countries, processing 5 billion events per day.\textsuperscript{55})

This information can then be used to target individuals. For example anti-abortion activists use geo-fencing to target online ads at women as they enter abortion clinics.\textsuperscript{56} Near has reported that it could target individuals with messaging about the Australian Government’s COVIDSafe app: “We can support app adoption, saying to someone you’ve been to a postcode or a high-risk area and encourage them to download the app. That’s quite easy to do”.\textsuperscript{57} This is despite the company’s claim that its data is “anonymized to protect privacy”.

The New York Times’ Privacy Project used publicly available information about people in positions of power, linked with a dataset of location data drawn from mobile phone apps. The dataset included 50 billion location pings from the phones of more than 12 million Americans in Washington, New York, San Francisco and Los Angeles. The result was highly invasive:

“We followed military officials with security clearances as they drove home at night. We tracked law enforcement officers as they took their kids to school. We watched high-powered lawyers (and their guests) as they traveled from private jets to vacation properties. … We wanted to document the risk of underregulated surveillance. …Watching dots move across a map sometimes revealed hints of faltering marriages, evidence of drug addiction, records of visits to psychological facilities. Connecting a sanitized ping to an actual human in time and place could feel like reading someone else’s diary.”\textsuperscript{58}

Amendments to the Californian privacy law, which were passed by referendum earlier this month, will have the effect of adding geolocation data into the list of sensitive personal

\textsuperscript{52} David Pierce, “Location Is Your Most Critical Data, and Everyone’s Watching”, Wired, 27 April 2015; available at https://www.wired.com/2015/04/LOCATION/
\textsuperscript{53} See https://blog.near.co/news/workers-tracked-20km-from-infected-abattoir/
\textsuperscript{54} See https://blog.near.co/news/we-know-which-suburb-eats-more-pizza-by-analyzing-data-from-15-million-australians/
\textsuperscript{55} See https://near.co/data/
\textsuperscript{57} See https://blog.near.co/news/workers-tracked-20km-from-infected-abattoir/
information, and thus require more stringent protective measures.\textsuperscript{59} We submit that Australian privacy law should also recognise the particularly intrusive nature of location data, if not in the definition of ‘sensitive personal information’ then by way of a ‘no-go’ zone within an overarching fairness framework.

A final example of a ‘no-go’ zone should be the collection or use of biometrics, including facial recognition technology, except in extremely limited and explicitly legislatively authorised circumstances. We note that in late 2019 the Australian Human Rights Commission (AHRC) recommended a moratorium on the use of facial recognition technology.\textsuperscript{60} We support that recommendation, and note that a number of jurisdictions have introduced moratoria on the use of facial recognition technology in 2020 in response to two significant developments.

The first was the death of George Floyd in May 2020, which triggered not only global Black Lives Matter protests, but an unprecedented degree of self-reflection on the role of racial profiling in policing. The effects have spilled over into Big Tech and ethical debates over the use of facial recognition technology.\textsuperscript{61}

The second was revelations about the disturbing data collection and sales practices utilised by Clearview AI. Documents released under FOI show that the Australian Federal Police used the technology as part of a free trial (contrary to their initial denials),\textsuperscript{62} and that Victoria Police did likewise, without authority.\textsuperscript{63} The Victorian documents contained an email from Clearview AI to a police sergeant, encouraging them to “feel free to run wild with your searches” to see what comes up, such as by trying the system on their friends, family or a celebrity.\textsuperscript{64}

Clearly existing privacy laws have failed to prevent either extensive compilations of biometric data by private sector companies simply ‘scraping’ data from the internet, or the use of such technologies by our own police forces without proper procurement processes or regulatory (let alone public) scrutiny.

Purported consent should not be allowed as the lawful basis on which such practices can flourish. Under a truly effective model of privacy regulation, the hard choices about limiting the use of personal information, protecting autonomy and dignity, and avoiding privacy harms, must be made well before the individual user, consumer or citizen ever becomes involved. An overarching ‘fairness framework’ is needed instead.

\textsuperscript{59} The California Privacy Rights Act 2020 expands the definition of ‘sensitive personal information’ (which is afforded superior protection) to include “a consumer’s precise geolocation”, which is defined as “any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet”; see https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf
\textsuperscript{61} IBM was the first company to step back from their own business practices, promising that it would no longer offer, develop or research facial recognition technology. This was shortly followed by Amazon setting a one year moratorium on the use of their technology by law enforcement, in the expectation that Congress would create ethical rules for facial recognition technology. Then Microsoft jumped on the bandwagon with a press release noting that it would not sell its technology to law enforcement agencies until there is a federal law regulating facial recognition technology.
\textsuperscript{64} See https://drive.google.com/file/d/1s_MWdF8AlQAHQhxXve5Ve6EKXwcG_q/view
Strengthen the APPs

We submit that the objective of the Privacy Act should be to restrict data flows (i.e. the collection, use and disclosure of personal information) unless they can be justified within a framework of overarching principles including necessity, proportionality and fairness.

First, the Accountability principle, APP 1, should be strengthened. To bring the Privacy Act into line with the GDPR, APP 1 should be amended to introduce:

- A requirement for APP entities to implement the remaining privacy principles ‘by design and by default’.\(^{65}\) We note here that the ACCC recommended in its Customer Loyalty final report that default settings should be ‘off’ to unnecessary purposes such as marketing.\(^{66}\)

- A requirement for APP entities to conduct Privacy Impact Assessments (PIAs) on inherently ‘high risk’ projects. We note that this is already the case for Australian Government agencies under the Code made under APP 1; we submit that the same requirement should apply to the private sector.

- A requirement for APP entities to report to the OAIC when projects have a residual ‘high risk’ (i.e. where the PIA Report concludes that even after recommended mitigation strategies or risk controls are adopted, the project will remain ‘high risk’); with the OAIC being granted powers to require the project to cease or not proceed\(^{67}\)

Second, tighten up the collection limitation principle, APP 3. Although APP 3.5 already requires the means of collection to be ‘lawful and fair’, this could be placed more ‘up front’ in APP 3, along with the need to ensure that personal information is only collected when it is fit for purpose. The requirement that collection be ‘lawful and fair’ should also extend to the nature of the data collected, not just the means by which it is collected. (See also discussion above in relation to an overarching ‘fairness framework’.)

We note that the ACCC, in its Customer Loyalty inquiry, found examples of the collection of personal information in circumstances in which the consumer would not have been aware (and indeed would likely have run directly counter to their expectations), such as customer loyalty schemes which tracked transactions even when the customer did not proffer their card.\(^{68}\) This type of collection should be clearly prohibited under APP 3. (Also see further discussion below about the collection of personal information in the context of online behavioural advertising.)

Third, give transparency rules teeth, by linking use or disclosure under APP 6 to the requirement to first provide clear notice under APP 5. Californian privacy law directly ties

---

\(^{65}\) See Article 25 of the GDPR.


\(^{67}\) See Articles 36 and 58 of the GDPR.

collection limitation and use limitation to transparency in this way; see clause 1798.100(b) of the CCPA, which provides:

“A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.”

Fourth, tighten the rules on use and disclosure. No doubt some submissions will suggest that APP 6 should be re-framed to more closely mirror Article 6 of the GDPR, which has six grounds on which personal data can be lawfully ‘processed’ (collected, used or disclosed), including a ‘legitimate interests’ ground. However in our view APP 6 needs only minor tweaks to achieve a standard more suitable for contemporary times.

We submit that APP 6 should be amended such that:

- primary purpose is defined as the primary purpose of the original collection as notified to the individual (and not the entity’s self-serving notion of its own ‘primary purpose’)
- the related secondary purpose test to be “directly related to, and reasonably necessary to support, the primary purpose”
- the ‘directly related secondary purpose’ test is applied to sensitive personal information and non-sensitive personal information alike, so as to avoid overly generous self-serving claims by APP entities about the extent to which secondary purposes, which are only indirectly ‘related’, are authorised under APP 6.

Fifth, the Data Quality principle, APP 10, should be strengthened. The ‘Robodebt’ scandal illustrates how decision-making involving personal information that was simply not fit for the intended purpose has cost the government $1.2 billion thus far. The information supplied to Centrelink from the Australian Taxation Office may well have been accurate, up-to-date and complete (the existing test under APP 10); but in the context of the purpose to which Centrelink planned to use it, it was misleading, and neither fair nor fit for purpose.

We submit that APP 10 should be amended, such that for collection, use and disclosure, the APP entity must – in addition to the existing requirements that the personal information be accurate, up-to-date and complete - also ensure that the personal information is relevant, not misleading, fair and fit for its intended purpose.

---

Regulate direct marketing and online targeting

The Issues Paper asks the following question:

- Does the Act strike the right balance between the use of personal information in relation to direct marketing? If not, how could protections for individuals be improved?

APP 7 regulates the use and disclosure of personal information for direct marketing, in circumstances in which the Spam Act or Do Not Call Register Act do not already apply.

APP 7 does not regulate collection for direct marketing purposes, yet in the online environment arguably the most intrusive conduct in the name of marketing occurs at the points of collection, and collation to generate profiles. (Our comments above in relation to online identifiers and the definition of personal information, the ‘legal fiction’ of consent-based practices, and unfair collection practices, are all also relevant to any discussion of the collection or use of personal information for direct marketing.)

In his keynote speech at the 2019 IAPP ANZ Summit, Privacy Commissioner of New Zealand John Edwards noted Facebook’s response to the ACCC’s recommendations around making online behavioural advertising opt-in only, which was to the effect that implementation would “make targeted advertising practically unworkable”. Edwards said:

“maybe some kinds of ‘targeted advertising’ should be ‘practically unworkable’ – especially if they are deeply intrusive, there’s no meaningful consent and there’s no way to opt out. We know that Facebook offers thousands of different market segmentations that advertisers can target. These can be explicitly racist or divisive, such as allowing advertisers to target self-declared or inferred ‘Jew-haters’, or through a myriad of proxies facilitated through thousands of seemingly innocent data points.”

In January 2020 the Norwegian Consumer Council (NCC) released a report analysing third party data sharing from 10 popular apps. The NCC analysed data traffic from ten popular apps such as dating apps and period trackers, which were found to transmit user data to at least 135 different third parties which then used the collected data to generate consumer profiles for targeted advertising. The report noted that some apps were found to be sharing information about sexuality, drug use and political views, and collating data to infer religion and sexuality. The NCC states:

“every time we use our phones, a large number of shadowy entities that are virtually unknown to consumers are receiving personal data about our interests, habits, and behaviour … the digital marketing and adtech industry, use this information to track us over time and across devices, in order to create comprehensive profiles about individual consumers. In turn, these profiles and groups can be used to personalize

and target advertising, but also for other purposes such as discrimination, manipulation, and exploitation”.

As the dangers of online behavioural advertising are becoming clearer, there are significant shifts in community sentiment towards direct marketing, as well as efforts by privacy regulators and legislators, and even Big Tech themselves, to rein in the online advertising and data broking industries.

For example under Californian privacy law, different standards have been set in relation to data collection about children for marketing purposes: in circumstances where for adults the standard is opt-out, for children it is set to opt-in (which is to be exercised by parents for under 13s, or by children themselves aged 13-16).

Google is phasing out the use of third party cookies on its Chrome browser by 2022; Mozilla’s Firefox and Apple’s Safari browsers had already moved to ban third party cookies. Apple’s iOS14 is being used to roll out a system of opt-in only for tracking users across different apps and websites.

The combination of the GDPR and the ePrivacy Directive has meant that consent is required for the placement of third party cookies on a user’s device, or other forms of online monitoring. Those requirements are now being enforced via court decisions and privacy regulators’ investigations which have interpreted the essential elements of consent more strictly than the industry would like. The UK’s ICO has also proposed regulation if the online behavioural industry doesn’t self-regulate, noting “It is unlikely that you will be able to apply legitimate interests for intrusive profiling for direct marketing purposes”.

There are also calls to make targeted marketing and profiling opt-in only, by law. For example in October 2020, Members of the European Parliament voted 637 to 26 in favour of a resolution to develop laws to phase out personalised or targeted online behavioural advertising, starting with enabling consumers to opt-out, but leading eventually to a complete ban.

However any regulation in this space must distinguish between the more intrusive and covert tracking and profiling activities which power online behavioural advertising at one end of the scale, and a business sending out an email or hard copy newsletter to its existing customer base on the other.

---


We submit that the actual delivery of direct marketing to an individual with whom an organisation has a pre-existing relationship should remain lawful, on an opt-out basis. This would include individuals such as a past customer, or someone who has made an enquiry of the business or who has taken up an offer such as to subscribe to a newsletter.

However marketing by third parties, or the use of second party or third party customer data via online behavioural advertising, should be prohibited.

We submit that the scope of APP 7 is no longer fit for purpose: its scope is too narrow to encompass the privacy harms posed by the use of online identifiers and other individuation techniques to directly contact individuals. In the digital economy, business practices go beyond the marketing of goods and services to also include automated decisions about the goods or services offered to a customer in the first place, automated decisions about prices offered to a customer, personalised content and political messaging.

We submit that the following amendments should be made to the Privacy Act, to better regulate direct marketing and similar online targeting activities that occur in the digital environment:

a) Repeal APP 7

We submit that instead, APP 6 should cover the field for determining whether or not profiling and/or contacting an individual is appropriate. Direct marketing and similar activities would thus typically fall under APP 6.2(a) – the ‘related secondary purpose’ test. (This suggestion would not affect the operation of the Spam Act or Do Not Call Register Act, which regulate the use of particular communication channels.)

b) In APP 6, prohibit disclosure for the purpose of direct marketing, messaging, profiling, targeting or tracking individuals (whether online or offline) under the ‘related secondary purpose’ test

This provision would halt the trade in personal information between different entities seeking to engage in data sharing or data-matching for the purpose of online behavioural advertising or other forms of direct marketing, messaging, profiling, targeting or tracking, unless another exception applied, such as ‘with the consent of the individual’ (or law enforcement, public interest research, etc).

By limiting this requirement to practices otherwise authorised under the ‘related secondary purpose’ test, this requirement would not be imposed unnecessarily on practices covered by other parts of APP 6 or other laws, such as a telecommunications provider disclosing location data to law enforcement for the purpose of tracking a suspect.
This provision would not impact the provision of customer data to a third party contractor such as a mailing house, because the provision of data to a contracted service provider would not constitute a ‘disclosure’ but a ‘use’.

c) In APP 6, prohibit any use of ‘sensitive personal information’ for direct marketing, messaging, profiling, targeting or tracking of individuals (whether online or offline) under the ‘related secondary purpose’ test.

This provision would replicate APP 7’s requirements that the use of sensitive personal information for direct marketing requires the consent of the individual. This is also consistent with the Canadian and European approaches.

By limiting this requirement to practices otherwise authorised under the ‘related secondary purpose’ test, this requirement still allows for use under another exception, such as ‘with consent’.

d) In APP 6, require all use of personal information for direct marketing, messaging, profiling, targeting or tracking of individuals (whether online or offline) under the ‘related secondary purpose’ test to include a clear, accessible and functional opt-out (aka unsubscribe) mechanism; and prohibit direct marketing, messaging, profiling, targeting or tracking individuals (whether online or offline) if the individual has opted-out.

This provision would replicate the position now in relation to direct marketing (whether considering APP 7 or the Spam Act), but extend it to other forms of direct messaging, profiling, targeting or tracking of individuals.

Similar to the ‘unsubscribe’ link on an email newsletter, online behavioural advertising or political targeted messaging (as opposed to contextual advertising) should be clearly identified to the user as an ad or message shown to this user, along with a mechanism providing that user with the opportunity to easily opt out of all such future direct marketing, messaging, profiling, targeting or tracking.

This position is consistent with the Canadian approach of allowing most forms of online behavioural advertising, so long as individuals can easily opt out. The effect would be to prohibit practices which do not support user control, such as zombie cookies.

By limiting this requirement to practices authorised under the ‘directly related secondary purpose’ test, this requirement would not be imposed unnecessarily on practices covered by other parts of APP 6 or other laws, such as law enforcement tracking of a suspect; or a telecommunications provider recording geolocation data as part of their primary purpose of delivering a mobile phone service.
Other permitted purposes

The Issues Paper also asks the following question:

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

It is our submission that the exemptions for research, currently found in sections 16B, 95 and 95A of the Privacy Act, ought to be re-considered and re-drafted. We submit that the essential conditions for allowing research to proceed should be similar: i.e. that an appropriately-constituted human research ethics committee has approved of the proposed collection, use or disclosure of personal information as necessary for a research project which is in the public interest, the expected benefits of which outweigh the public interest in the maintenance of privacy protections. The committee must also still be required to attest that a waiver of individual consent is necessary (otherwise the project must proceed only on the basis of participant consent), and must determine whether or not the research project can be conducted using de-identified data instead of personal information.

However we also believe that the scope of the two exemptions is too narrow, and that the distinction between public sector and private sector application is an unnecessary hangover from the pre-2014 structure of the Act.

Section 95 regulates personal information held by the public sector, and creates an exemption to all the APPs, but only in relation to medical research. By contrast s.95A regulates personal information held by the private sector, and creates an exemption to the collection, use and disclosure principles, for any type of research “relevant to public health or public safety”, but only in relation to health information.

Thus personal information held by Australian government agencies cannot be used to conduct non-medical research, such as research into the financial effects for working mothers of altering childcare rebates, or research into the educational outcomes achieved by changing tertiary education funding.

Meanwhile private sector organisations cannot use non-health personal information in research projects, even if those projects are highly relevant to public safety, such as research into better designing personal protective gear to fit the different body shapes of a workforce.

Both current exemptions fail to give due consideration also to the steps preliminary or ancillary to the conduct of the research itself, such as the steps involved in participant identification and recruitment.77

---

77 See ‘PA and Department of Veterans’ Affairs (Privacy) [2018] AICmr 50 (23 March 2018) for an example of a case in which the OAIC had to stretch the literal meaning of s.95 to allow for the participant recruitment phase to fit within the umbrella of the research exemption; available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2018/50.html
We work with many clients in the research and data analytics space, in both the public and private sector, and we have often found the drafting of s.95 and s.95A to prohibit research that would otherwise have a high public interest value. By contrast other privacy laws at the State and Territory level do not artificially constrain the scope of their research exemptions.

We submit that s.95 and s.95A should be repealed, and replaced with a single exemption, the scope of which includes (as relevant and necessary to each project) the collection, use or disclosure of any types of personal information (not just health information), for research projects in the public interest (not just medical research), including the steps preliminary or ancillary to the actual research (such as participant identification and recruitment, and the process of applying de-identification techniques to the data).

Inferring sensitive information

The Issues Paper asks the following question:

- Does the definition of ‘collection’ need updating to reflect that an entity could infer sensitive information?

The OAIC has issued guidance to suggest that the creation of new data, such as by generating new inferences about an individual from existing data, will constitute a ‘collection’, such that the limitations and requirements of APPs 3 and 5 apply. We submit that this position should be made explicit in the legislation itself, so as to leave no doubt about the scope of the Collection principles. However this issue is not limited to sensitive personal information.

Individual rights

The Issues Paper asks the following question:

- Should a ‘right to erasure’ be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?

We note first that the OAIC’s guidelines suggest that APP 13, the right to Correction, already can include deletion, where appropriate.78 We submit that this should be made explicit within the statute itself, by way of amendment to APP 13.

We also note that both the CDR scheme and the My Health Records Act have a “right to deletion on request”, and that the CCPA also has a right to erasure with exemptions worth reviewing.

---

78 See part 13.47 of the OAIC’s Guidelines to the APPs, July 2019.
However in our view, while considering the adoption of GDPR-style individual subject rights, a much more significant improvement could be achieved by adding to the Privacy Act:

- a right to human review of automated decision-making, and
- a right to algorithmic transparency.

Such rights would not only help to protect vulnerable individuals, but would help protect governments and businesses against their own poor decision-making, such as we saw with the design of ‘Robodebt’.

We note that the Bill just laid before the Canadian Parliament to update the Canadian privacy laws includes a new right to algorithmic transparency.79

We also note that the AHRC recently recommended the need for regulation to ensure fairness and transparency in the use of artificial intelligence (AI), in order to promote ‘responsible’ innovation, that is ethical, lawful, fair, transparent and safe.80 We support those recommendations.

We further submit that a detailed framework for ensuring algorithmic fairness and responsible use of personal information in AI should be fleshed out as a Code under APP 10 (Data Quality).

---

79 If enacted, section 63 of the Consumer Privacy Protection Act (Canada) will add to the existing Access and Correction rights the following requirement: “If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision and of how the personal information that was used to make the prediction, recommendation or decision was obtained”. Organisations will also be required, under s.62, to include details of their use of automated decision systems in their Privacy Policies. “Automated decision system” is defined in the Bill to mean “any technology that assists or replaces the judgement of human decisionmakers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets”. See https://parl.ca/Content/Bills/432/Government/C-11/C-11_1/C-11_1.PDF

Penalties

We note that the CDR scheme has significantly higher penalties for a breach of a Privacy Safeguard than does the Privacy Act. The CDR penalties are set at whichever is highest out of $10M, 10% of domestic turnover pa, or three times the value of benefits obtained from the breach.

We submit that civil penalties under the Privacy Act, to be levied by the OAIC, should be increased to mirror the CDR scheme.

A direct right of action

The Issues Paper asks the following questions:

- How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

Privacy principles are meaningless if they cannot be enforced.

As noted by the Issues Paper, there is no ability for an individual to appeal from a decision by the Commissioner to dismiss a complaint. While there is merit in having a gatekeeper to prevent unmeritorious complaints, in reality the effect is to put the OAIC in the role of both bottle-neck (there are significant delays in complaints being allocated a case officer) and road-block. This significantly impacts on access to justice. We have seen complaints which in our view had merit simply dismissed by the OAIC without even proceeding to a s.52 determination, where the respondent and complainant disagreed about interpretation of an APP in a matter of significance, i.e. where a ruling on the matter would have had much broader application than just the complainant’s case.

Further, appeals against any formal determinations by the OAIC must be heard in the Federal Court, which exposes individuals to extensive costs. This is the reason there is so little case law found interpreting the Privacy Act.

We note that a statutory right to sue for damages has already been introduced in Australia under the CDR scheme, in relation to any breach of a Privacy Safeguard in relation to CDR data. The CCPA also creates a statutory right to sue for (capped) damages for a data
breach, for some specific types of personal information, in cases where the respondent did not have reasonable data security (CCPA clause 1798.150).

Further, a successful class action in NSW in 2019 suggests that ‘breach of confidence’ can work as a path through which victims of a data breach can sue for damages under common law. We submit that a statutory scheme with a cap on damages would be preferable.

We therefore submit that a direct right of action, via an accessible and cheap tribunal, is essential to deliver meaningful privacy protections to everyday Australians.

We submit that the Privacy Act should be reformed to enable complainants the option of pursuing their argument about a respondent’s breach of the APPs (or other ‘interference with privacy’ as defined under the Privacy Act) in a tribunal which defaults to no-costs basis hearings. This could be established such that the right to lodge a case in the tribunal is only triggered if the complainant has first tried to pursue informal settlement, either directly with the respondent or indirectly via the OAIC, and a certain time period has since lapsed without an outcome to their satisfaction. The right should not be prevented if the matter has resulted in a dismissal or unfavourable determination by the OAIC.

NSW offers a model for accessible justice in relation to privacy complaints. Since the Privacy and Personal Information Protection Act 1998 (NSW) commenced in 2000, there have been over 460 privacy cases reported. While by no means a perfect system, the NSW Civil and Administrative Tribunal offers complainants an opportunity to be heard, without needing legal representation or being exposed to costs orders. Cases may only be lodged if the complainant has first sought an ‘internal review’ by the respondent, and either the internal review was not completed within 60 days, or the complainant was dissatisfied with the result. The NSW Privacy Commissioner is notified of each internal review, and has the right to appear as amicus curiae in the Tribunal. The vast majority of cases which result in compensation are at the low end of the scale, typically less than $10,000.

A federal tribunal should have a maximum limit of compensation which is meaningful for a complainant who has suffered significant financial, physical or psychological harm, but without placing undue burden on businesses, such as $150,000.

---

A statutory tort of privacy

The Issues Paper asks the following questions:

- Is a statutory tort for invasion of privacy needed?
- Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?
- What types of invasions of privacy should be covered by a statutory tort?

We submit that a statutory tort for invasion of privacy is needed, and should be developed in line with the Australian Law Reform Commission’s detailed proposal. A tort has been recommended over and over again by a number of regulators, as well as independent and bi-partisan bodies. There is no need to re-litigate the question of necessity.

The following offer examples of serious invasions of privacy for which the victims should have been able to seek compensatory damages for the harm suffered, but which they were prevented from seeking under current privacy laws:

- revenge porn activities by individuals not operating a business; individuals are not bound by the APPs, and criminal offences in relation to non-consensual sharing of intimate images do not offer remedies to victims
- breaches caused by employees misusing their access to personal information about an organisation’s customers / patients / students / prisoners / other employees, but for which the employer is not liable because it was a misuse for a personal purpose, such as blackmail or in family court proceedings
- malicious breaches where the financial harm suffered exceeds statutory compensation limits (such as any caps introduced under a direct right of action, see above)

We further submit that the ALRC model should be adopted, with one caveat. Where the ALRC’s proposal included that the tort should include a defence that the defendant’s conduct was “required or authorised by law”, we suggest that this be amended to only cover conduct “required by law”.

Our concern is that including “authorised by law” as a defence is too broad, and could be used to shield egregious invasions of privacy. The tort should be drafted such that there should be no defence for privacy harms caused by activities which might be considered

---


83 See for example the case of NK v Northern Sydney Central Coast Area Health Service (No.2) [2011] NSWADT 81, available at https://www.caselaw.nsw.gov.au/decision/54a6345130044de94513d65ef
exempt or ‘allowed’ under existing privacy statutes, but which have nonetheless caused harm because the activity in question was negligent, malicious or corrupt.

Examples include:

- a negligent or reckless failure to check a child protection allegation which the police “know is false or should reasonably be expected to know to be false” before acting on it\(^{84}\)
- systemic problems like a failure to ensure the accuracy of bail records, so that hundreds of children end up wrongly arrested or imprisoned,\(^{85}\) and
- a failure to enforce data retention rules, so that decades-old ‘spent’ convictions are disclosed to a man’s partner and employer.\(^{86}\)

Each of the above examples impacted individuals in serious ways. They should have been able to pursue compensation for the harms they suffered. However because of an exemption\(^{87}\) intended to protect legitimate law enforcement conduct by NSW Police and other agencies, but which through poor legislative drafting has also been found to also shield illegitimate conduct, any ability for these victims to seek a remedy has been blocked.

Please note that many of the above examples have arisen in NSW caselaw, rather than cases brought under the Privacy Act. We submit that it is because of the lack of a direct right of action under the Privacy Act (as discussed above) that equivalent complaints about Australian Government agencies and the private sector do not even come to light.

---


About the author

This submission was prepared by Anna Johnston, Principal, Salinger Privacy.

Anna has served as:

• Deputy Privacy Commissioner of NSW
• Chair of the Australian Privacy Foundation, and member of its International Committee
• a founding member and Board Member of the International Association of Privacy Professionals (IAPP), Australia & New Zealand
• a member of the Advisory Board for the EU’s STAR project to develop training on behalf of European Data Protection Authorities
• a Visiting Scholar at the Research Group on Law, Science, Technology and Society of the Faculty of Law and Criminology of the Vrije Universiteit Brussel
• a Member of the Asian Privacy Scholars Network
• a member of the Australian Law Reform Commission’s Advisory Committee for the Inquiry into Serious Invasions of Privacy, and expert advisory group on health privacy, and
• an editorial board member of both the Privacy Law Bulletin and the Privacy Law & Policy Reporter.

Anna has been called upon to provide expert testimony to the European Commission as well as various Parliamentary inquiries and the Productivity Commission, spoken at numerous conferences, and is regularly asked to comment on privacy issues in the media. In 2018 she was recognised as an industry leader by the IAPP with the global designation of Fellow of Information Privacy (FIP).

Anna holds a first class honours degree in Law, a Masters of Public Policy with honours, a Graduate Certificate in Management, a Graduate Diploma of Legal Practice, and a Bachelor of Arts. She was admitted as a Solicitor of the Supreme Court of NSW in 1996. She is a Certified Information Privacy Professional, Europe (CIPP/E), and a Certified Information Privacy Manager (CIPM).
About Salinger Privacy

Established in 2004, Salinger Privacy offers privacy consulting services, specialist resources and training.

Our clients come from government, the non-profit sector and businesses across Australia. No matter what sector you are in, we believe that privacy protection is essential for your reputation. In everything we do, we aim to demystify privacy law, and offer pragmatic solutions – to help you ensure regulatory compliance, and maintain the trust of your customers.

Salinger Privacy offers specialist consulting services on privacy and data governance matters, including Privacy Impact Assessments and privacy audits, and the development of privacy-related policies and procedures. Salinger Privacy also offers a range of privacy guidance publications, eLearning and face-to-face compliance training options, and Privacy Tools such as templates and checklists.

Qualifications

The comments in this submission do not constitute legal advice, and should not be construed or relied upon as legal advice by any party. Legal professional privilege does not apply to this submission.