Dear OAIC,

Thank you for the opportunity to contribute to the Children's Privacy Code of Conduct.

For Children's privacy online to be effective existing encumbrances presented by the existing legal precedent means that Children Online Privacy cannot be effective until this is rectified by the Parliament.

The Privacy Act, is very reliant upon presenting the intent of the parliament to a court, in order to see community expectations regarding information privacy met, this has not occurred and is very difficult and would be exceptionally expensive. The ALRC reports total in excess of two thousand, two hundred pages.

Additionally, the parliament's intent is documented in parliamentary debates and 2nd reading speeches – failure to identify and present the purpose from these 2nd reading speeches and you risk loosing your case. The Commonwealth Government has intended on two occasions for the Privacy Act to deal with online privacy issues.

The Commonwealth provide no obvious change to the Privacy Act to reflect this intent, unlike the Western Australian Government which has clearly put it's intention into in the PRIS Act by defining personal information to include:

> (b) means information or an opinion, whether true or not, and whether recorded in a material form or not, that relates to an individual, whether living or dead, whose identity is apparent or can reasonably be ascertained from the information or opinion; and includes information of the following kinds to which paragraph (a) applies —
>
> (i) a name, date of birth or address;
>
> (ii) a unique identifier, online identifier or pseudonym;
>
> (iii) contact information;
>
> (iv) information that relates to an individual's location;
>
> (v) technical or behavioural information in relation to an individual's activities, preferences or identity;
>
> (vi) inferred information that relates to an individual, including predictions in relation to an individual's behaviour or preferences and profiles generated from aggregated information;
>
> (vii) information that relates to 1 or more features specific to the physical, physiological, genetic, mental, behavioural, economic, cultural or social identity of an individual;

Had the Commonwealth done so, then I'd like to this a very different decision would have been reached in key cases, like the Grubb cases that I'll mention later.

This has severely inhibited the development of our understanding of information privacy in Australia.

The Parliament has to recognise the reality of the modern practice of law and the courts, it must embed key concepts, interpretations into the Act. The only people who will sift through the thousands of pages of material are law students with an assignment and/or activists who are trying to make a better world.

For Parliament to relying upon these people to find the authorities for interpretations of the Act is negligent.

The current act would also require Australia's Privacy regulators need to lift their game, first year law students are taught that acts have no unnecessary words (the principle of non surplusage), which the Full Federal Court[1] relied upon to dismiss an appeal by the OAIC.

The other key challenge, is that protecting other people's privacy requires me to go out of my way for little benefit to me, there is talk of privacy being good for trade; however with no stick, there is no incentive to drive the right behaviours.

Sincerely,

[REDACTED]

[1] *Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4* [62].

History of Privacy in Australia.

Until very recently, the leading decision in relation to Privacy was 'you should build a higher fence'[2], with changes arriving in 2001[3].

This decision was made some 13 years after the passing of the (Information) Privacy Act (Cth). Additional aspects of privacy are dealt with by laws that cover recording what people are doing, or 'surveillance device act' laws, which were updated from 'listening device' acts. Human Rights, where charters have been enacted also play a part, as they protect privacy and correspondence.

There are also privacy indicators in other laws, such as Part 13 of the Telecommunications Act, which states location of a mobile handset relates to the 'affairs of the customer responsible for the handset or device'[4].

There have also been a number of inquiries or reports into Privacy.

- ALRC Report 22 – Privacy, 1983.
- ALRC Report 108 – For Your Information: Australian Privacy Law and Practice
- ALRC Report 123 – Serious Invasions of Privacy in the Digital Era.
- ACCC Digital Platforms Inquiry
- The Victorian Parliament's inquiry into Computers and the Law.

The relevant Government typically provides a response to the report, which may also be mentioned in the second reading speeches when updates to Acts are passed.

These laws or inquiries were often preceded by an International Treaty or similar, including the OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data and the International Conventant on Civil and Political Rights. Protecting Privacy is also considered to be good for trade. This is reflected in a number of 2nd reading speeches by former Attorney Generals Roxon and Williams when updating the Privacy Act[5][6]. Interestingly in both of these speeches mentioned the desire for the privacy act to address online privacy concerns.

Ultimately, for the Children's Privacy Code to be effective, challenges with the privacy act itself need to be resolved, and this includes supporting legislation at the state level.

Success will also depend on uniform national laws for some matters that are currently legislated by the states, e.g. surveillance devices acts, electronic transactions acts. These complex interaction between all these laws will need to be supplemented by appropriate skilled legal professionals and specially trained courts.

---

[2] *Victoria Park Racing v Taylor (1938) 58 CLR 479*.
[3] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd [2001] HCA 63*.
[4] *Telecommunications Act 1997 (Cth)* s275A.
[5] 'Commonwealth, Parliamentary Debates - Privacy Amendment (Enhancing Privacy Protection) Bill 2012, House of Representatives, 23/5/2010 N Roxon, Attorney-General)'.
[6] 'Commonwealth, Parliamentary Debates - Privacy Amendment (Private Sector) Bill 2000, House of Representatives, 12/4/2000 (D Williams, Attorney-General)'.

An alternative is the EU's approach with the directives informally known as the ePrivacy Directive[7][8][9] (cookie laws). These directives were recently upheld in EU[10], despite significant pressure and push back from the Information Technology Sector.

There is also a need in Australia to confirm whether or not existing juris prudence on technological issues is correct, stemming from the Grubb matter[11], which was appealed to the AAT[12] and then the Full Federal Court[13]. Notably the OAIC claimed[14] its interpretation of the Privacy Act and what is personal information was correct; however the situation is quite confusing as Tribunals have both accepted[15] and rejected[16] the AAT's position.

Given the above, I think the Western Australian Government, has wisely included clarifying information in Privacy and Responsible Information Sharing Act of 2024, as follows:

> includes information of the following kinds to which paragraph (a) applies —
> (i) a name, date of birth or address;
> (ii) a unique identifier, online identifier or pseudonym;
> (iii) contact information;
> (iv) information that relates to an individual's location;
> (v) technical or behavioural information in relation to an individual's activities, preferences or identity;
> (vi) inferred information that relates to an individual, including predictions in relation to an individual's behaviour or preferences and profiles generated from aggregated information;
> (vii) information that relates to 1 or more features specific to the physical, physiological, genetic, mental, behavioural, economic, cultural or social identity of an individual.

Throughout this paper, I will identify additional areas or concepts that could be clarified by strengthening the Privacy Act, rather than relying upon international treaties, ALRC reports, 2nd reading speeches, etc. These also should make the benefits of the Privacy Act and Children's Privacy Code more 'accessible' and avoid complex and costly legal argument.

---

[7] *Directive 2009/136/EC*.
[8] *Directive 2002/58/EC*.
[9] *Directive 2002/22/EC*.
[10] *Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH [2019] ECLI:EU:C:2019:801*.
[11] *Ben Grubb and Telstra Corporation Limited [2015] AICmr 35*.
[12] *Telstra Corporation Limited and Privacy Commissioner [2015] AATA 991 (18 December 2015)*.
[13] *Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4* (n 1).
[14] 'Update on the Federal Court Decision' <https://web.archive.org/web/20170306182506/https://www.oaic.gov.au/media-and-speeches/statements/privacy-commissioner-v-telstra-corporation-limited-federal-court-decision>.
[15] *GMW v Victoria Legal Aid [2022] VCAT 922*.
[16] *Glass v Cessnock City Council [2024] NSWCATAD 292*.

Commentary on "What we've learnt so far".

Concerns about Privacy and a call for stronger protections

The quote here echoes what many people think - Privacy in Australia is not currently working as intended; and 3 Law Reform Commission Reports[17][18][19], combined with the ACCC's Digital Platforms Inquiry[20] support this view. There is much that can be learnt from our past, to make the best start moving forward.

There is no trust by website operators and/or businesses to be open and honest with consumers regarding what is going on in the background. When debating the Victorian Surveillance Devices Bill, the Victor Perton[21] talks about profiling of spending via credit cards, data surveillance devices, and the lack of trespass law in relation to our private selves. Why is there no trust ? It is not clear, perhaps it is as Victor Perton described it a lack of awareness by the Public as to what is going on.

The Victorian Parliament[22] intended for Information Privacy Bill in Victoria to address online privacy issues[23][24][25] (online monitoring tools, web bugs and cookies), however it has not. The Commonwealth Parliament has twice indicated[26][27] that it desired the Privacy Act be applied to online privacy issues.

The Act has not been interpreted this way, and is now hindered by the legacy of the Grubb cases[28][29][30]; following the Full Federal Court's decision, the Privacy Commissioner claimed that the approach taken to determining what is personal information by his office was correct[31]. This is not how the case has been applied in the Courts[32]. Additionally, the decision that information is not personal information because of short lived associations, is not consistent with privacy and the explanatory memoranda to OECD Guidelines on Transborder Data Flows, where the exposure of data in transit needs to be considered.

---

[17] 'ALRC Report 22 - Privacy' <https://www.alrc.gov.au/publication/privacy-alrc-report-22/>.
[18] 'Australian Law Reform Commission Report 108 - For Your Information: Australian Privacy Law and Practice'.
[19] 'Serious Invasions of Privacy in the Digital Era (ALRC Report 123)' <https://www.alrc.gov.au/wp-content/uploads/2019/08/final_report_123_whole_report.pdf>.
[20] 'Digital Platforms Inquiry' <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>.
[21] 'Victoria, Parliamentary Debates, Legislative Assembly, 22/4/1999 Hon. Victor Perton'.
[22] 'Victoria, Parliamentary Debates, Legislative Council, 26 October 2000, 733, (Jenny Mikakos)'.
[23] 'Web Bugs 1, Questions on Notice 29/2/2000 The Hon G Ashman.'
[24] 'Web Bugs 2, Questions on Notice 1/11/2000 The Hon V Perton.'
[25] 'Victoria, Parliamentary Debates, Legislative Assembly, 5/9/2000 Hon. Michael Leighton'.
[26] 'Commonwealth, Parliamentary Debates - Privacy Amendment (Private Sector) Bill 2000, House of Representatives, 12/4/2000 (D Williams, Attorney-General)' (n 6).
[27] 'Commonwealth, Parliamentary Debates - Privacy Amendment (Enhancing Privacy Protection) Bill 2012, House of Representatives, 23/5/2010 N Roxon, Attorney-General)' (n 5).
[28] *Ben Grubb and Telstra Corporation Limited [2015] AICmr 35* (n 11).
[29] *Telstra Corporation Limited and Privacy Commissioner [2015] AATA 991 (18 December 2015)* (n 12).
[30] *Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4* (n 1).
[31] 'Update on the Federal Court Decision' (n 14).
[32] *GMW v Victoria Legal Aid [2022] VCAT 922* (n 15).

While I agree with the Full Federal Court's obiter that points out ways in which the AAT's decision could have been wrong, I am concerned that some of the obiter[33] that is not harmonious with Part 13 of the Telecommunications Act 1997, which restricts the disclosure of the type of service provided[34], unlisted phone numbers, et al. The obiter regarding what is personal information appears inconsistent with the privacy principles related to direct marketing and more grounded in the 'personal affairs' version of 'personal information' rather than what was intended or required to meet our international treaty obligations.

This author's experiences in raising concerns with the OAIC this has not been the way the legal system has responded, cases have also sided with the AAT's interpretation[35] and the first case[36] I'm aware of that recognises the full federal court's obiter was decided late last year.

Until the definition of personal information is clarified, privacy will flounder as there is no way to 'get started'. The OECD Guidelines[37] which our Privacy Act was enacted to deliver on our international commitments define personal data as 'any information relating to an identified or identifiable individual'. This is reflected in ALRC's Report[38] as follows:

> "25.2 *Personal Information*. To limit the definition of 'personal information' to information relating to the 'personal affairs' of a person is too restrictive. Any information about a natural person should be regarded as being personal information. But the link between the person and the information need not be explicit. Information should be regarded as being 'personal information' if is information about a natural person from which, or by use of which, the person can be identified. Finally, the generally recommendations should not be restricted to personal information kept in a systematic fashion: in a record-system."

The above is how it was described by Attorney-General, Sir Lionel Bowen, in his second reading speech for the Privacy Act[39]:

> "'Personal information' is widely defined to include anything-act, true or false, or opinion-that reasonably identifies an individual."

The same conclusion can be reached from the Explanatory Memoranda to the Privacy Act 1988 (Cth); at least in Victoria, the Hon Jenny Mikakos was more direct in her restatement of this:

> "The definition of personal information goes beyond that to include, as I said earlier, an opinion or basically any information about an individual that is recorded in some form."

Additionally, in the ALRC has also discussed:

---

[33] *Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4* (n 1) [63].
[34] *Telecommunications Act 1997 (Cth)* (n 4) s270.
[35] *GMW v Victoria Legal Aid [2022] VCAT 922* (n 15).
[36] *Glass v Cessnock City Council [2024] NSWCATAD 292* (n 16).
[37] OECD, 'OECD Guidelines Governing The Protection of Privacy And Transborder Flows of Personal Data' <https://www.oecd.org/content/dam/oecd/en/publications/reports/2002/02/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_g1gh255f/9789264196391-en.pdf>.
[38] 'ALRC Report 22 - Privacy - Summary' 25.2 <https://www.alrc.gov.au/wp-content/uploads/2019/08/alrc22_summary.pdf>.
[39] 'Commonwealth, Parliamentary Debates - Privacy Bill 1988, House of Representatives, 1/11/1988 (L Bowen, Attorney-General)' p2117 <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F1988-11-01%2F0031%22>.

- The Interenet[40]
- Cookies[41]
- Web Bugs[42]

However little if any of this appears to have been (sufficiently well) communicated to the courts in any of the Grubb cases; nor was the desire of the Commonwealth Parliament for the Privacy Act to apply to online privacy issues as expressed in 2000[43] and again in 2012[44].

I commend the Western Australian Government in their approach to resolving this issue with the extension of the definition of personal information in the Privacy and Responsible Information Sharing Act:

"(b) includes information of the following kinds to which paragraph (a) applies —

(i) a name, date of birth or address;
(ii) a unique identifier, online identifier or pseudonym;
(iii) contact information;
(iv) information that relates to an individual's location;
(v) technical or behavioural information in relation to an individual's activities, preferences or identity;
(vi) inferred information that relates to an individual, including predictions in relation to an individual's behaviour or preferences and profiles generated from aggregated information;
(vii) information that relates to 1 or more features specific to the physical, physiological, genetic, mental, behavioural, economic, cultural or social identity of an individual;"

This should provide confidence for Western Australians and the Western Australian Government and save hours of court time.

I hope that the Australian Government sees the value in such clarification, and also in clarifying what is meant by 'privacy' and 'Information privacy'.

Transparency and age-appropriate communication

Privacy Policies (or collection statements) represent an agreement with the organisation and the person providing you with their personal information.

These agreements are seldom backed by appropriate management practices, I know of an organisation that promised to use the no-cookie based YouTube plugin on their website. However this was not backed by appropriate management practices; and the cookie based YouTube plugin was used on their website.

This reflects a lack of accountability for these policies and compliance with them; it also reflects inadequate communication between the privacy capability and ICT capability.

---

[40] 'Australian Law Reform Commission Report 108 - For Your Information: Australian Privacy Law and Practice' (n 18) Vol 1, p392.
[41] Ibid Vol1, p393.
[42] Ibid Vol 1, p394.
[43] 'Commonwealth, Parliamentary Debates - Privacy Amendment (Enhancing Privacy Protection) Bill 2012, House of Representatives, 23/5/2010 N Roxon, Attorney-General)' (n 5).
[44] 'Commonwealth, Parliamentary Debates - Privacy Amendment (Private Sector) Bill 2000, House of Representatives, 12/4/2000 (D Williams, Attorney-General)' (n 6).

The lack of confidence in these policies is reflected Brian Kreb's "We Take Your Privacy and Security. Seriously."[45] Many would rightly consider these documents as marketing material for which there is no consequence should they get it wrong.

Informed consent and digital literacy

I agree with the concerns raised here, in most cases the privacy offerings are 'take it or leave it' with no choices or benefits offered to the consumer; consent with other privacy agreements is assumed by website operators validly or otherwise.

Causing concern here is the lack of prominence of privacy notices, terms of use which could see a failure to meet the legal requirements for incorporation of terms by notice[46]. Few websites seem to take into account the various state based Electronic Transactions Acts which (correctly) reduce such notices to 'invitations to treat'[47].

What is meant by privacy varies significantly, the ALRC[48] noted the following privacy interests and related interests:

- Territorial Privacy – the interest in controlling entry to 'personal space';
- Privacy of the Person – the interest in freedom from interference with one's person and 'personal space';
- Information Privacy – the interest of the person in controlling the information held by others about him.
- Commications and Surveillance Privacy – freedom from surveillance, and from interception of one's communications; and
- Privacy of Attention – the ability to exclude intrusions that force one to direct attention to them rather than matters of one's one choosing.

There is very little education on privacy and information privacy rights; and Australia does not yet have a overarching Commonwealth bill of human rights, leading the way are states including Victoria and Queensland, along with the Australian Capital Territory. The Victorian Charter of Human Rights and Responsibilities Act, extends privacy to cover the family home and correspondence.

As mentioned earlier, the EU has taken the lead with online consent and simplified it with the privacy directives or cookie laws. Whether or not you agree with these directives, there is clarity for website operators.

Control over personal data and privacy

The desire for more control over their privacy and personal information is reflected in the concept of 'Information privacy'.

Regarding consent, it would appear that *express* consent is what is sought rather than *implied* consent, what is meant by explicit would need to be defined in this context. I certainly agree that people want to feel more in control over their personal information. I would also like to know what is meant by personal data, is it the same as personal information or something different

---

[45] 'We Take Your Privacy and Security. Seriously.' <https://krebsonsecurity.com/2014/09/we-take-your-privacy-and-security-seriously/>.
[46] *Thornton v Shoe Lane Parking Ltd [1971] 2 QB 163*.
[47] *Electronic Transactions (Victoria) Act 2000* s14B.
[48] 'ALRC Report 22 - Privacy - Summary' (n 38) p1.

(e.g. 'Information that relates to the plaintiff' per the Statutory Tort for Serious Invasions of Privacy) ?

The Privacy Act rightly doesn't require consent for the collection of personal information; there are practical considerations behind this. Taking photos in a public park would be very difficult if you needed to collect the consent of each person in the photo; however that may change should a photo or other recording be taken inside a building[49].

The Privacy Act, does however require that information is only collected by lawful and fair means (APP3.5) ; and that the information must be reasonably necessary for the organisations functions or activities (APP3.2).

So how does this work in practice ? When filling in forms, I would suggest that implied consent by filling in the form is usually what is relied upon. Where a state has surveillance devices laws that deal with recording what people are doing, those laws must also be complied with.

The online environment is quite complicated and discussed in an excellent paper by Dane McLeod – "Regulating Damage on the Internet: A Tortious Approach?"[50]. I prefer the approach taken by the EU with the *cookie laws*, as they are far more accessible to the legal profession, website operators and the general public.

It could be argued that people already have the ability to change their mind as to what they consent to – consent is typically not considered as 'consent in perpetuity'; however this would typically be limited to refusing to use a service. There are some websites that allow you to for example change your cookie preferences; however that is typically the limit of choice provided.

The 'right to be forgotten' or have actions forgotten is provided for in other countries, the addition of this or other rights would likely require additions or adjustments to the Australian Privacy Principles. Such adjustments would better reflect the views of contemporary Australians.

Data minimisation, privacy settings and geolocation data

Data Minimisation

Currently, data minimisation would be driven by APP 3.2, which allows for the collection of information that is reasonably necessary for one or more of the entity's functions or services.

This can be incredibly broad; and not restricted to the service being provided or a specific function being engaged.

This could be strengthened in two ways, firstly requiring that the information is strictly necessary and secondly by restricting the collection to be necessary to the service provided or as described in the collection notice.

If a 'strictly necessary' approach is taken, then I would suggest that this is made explicitly clear in the legislation; it could be argued that the Victorian Government intended for 'strictly necessary' based on the second reading speech of the Hon John Brumby[51], where he promised:

---

[49] *Surveillance Devices Act 1999 (Vic)* s7.
[50] Dane McLeod, 'Regulating Damage on The Internet: A Tortious Approach?' <https://classic.austlii.edu.au/au/journals/MonashULawRw/2001/14.pdf>.
[51] 'Victoria, Parliamentary Debates, Legislative Assembly, 26/5/2000 Hon John Brumby'.

> "It will protect the privacy of Victorians by giving people an assurance that only the minimum amount of personal information will be collected and that it will be held securely and used responsibly."

However the Supreme Court interpreted this to be 'reasonably necessary' by convention[52].

Privacy Settings

The code could mandate an 'opt-in' approach for privacy settings.

Based on cookies, this would likely spark debate as to what is 'necessary'; noting that cookies are not an essential part of a website, and certainly not a public website which doesn't require authentication to access.

Geolocation Data

If restricting the use of geolocation information is based on state surveillance devices laws, then efforts to ensure that the necessary provisions are in place would be needed. This is illustrated by the different definitions of tracking devices between the NSW and Victorian Acts:

> NSW: ***tracking device*** means any electronic device capable of being used to determine or monitor the geographical location of a person or an object.
>
> Vic: tracking device means an electronic device the primary purpose of which is to determine the geographical location of a person or an object;

The NSW Act suggests that consent is required to use any tracking device; where as in Victoria consent would only be required where it is the primary purpose of the device.

This also touches on another point, currently restrictions under Part 13 of the Telecommunications Act only apply to telecommunications carriers. They do not apply to website operators or similar, this provides another opportunity for providing clarity on the expectation of website operators.

Data security and protection from harm

Threat Environment

In Australia, we have the luxury of living in a society with low crime rates compared to other parts of the world. Physically attacking an Australian's in their home from another country is rendered unattractive through distance, border security measures including Australia's Military and our allies.

As a result, we have relatively modest home security controls.

The online threat environment is entirely different and much more like a war zone and has been for over twenty years, noting that in 2004 the 'survival time' of a unpatched PC connected to the internet without a firewall was just 16 minutes. Such attacks can be launched from anywhere on the globe and at very cost and low risk to the attacker and the owner of the device has very limited security controls.

Added to this, there is no equivalent of the security services provided in relation to Australia's Physical Borders.

---

[52] *Jurecek v Director, Transport Safety Victoria [2016] VSC 285; 260 IR 327* [103].

Data security

The commentary on data security is very light, authentication and encryption are two control groups.

Efforts in the data security space are expected to be particularly challenging because of the amount of 'change' required.

The use of a 'skimmer' as described in the penalty notice[53] issued by the UK ICO in relation to the hack of British Airways website illustrates that more is required than just authentication and encryption.

Security Frameworks like ISO 27001 have around 90 control groups, with thousands of individual controls if they are to be effective. As ISO 27001 allows organisations to choose their own controls, I would not recommend compliance with it in relation to this code.

The Open Web Application Security project's Application Security Verification Standard (ASVS) is well regarded publication in website security. The current version[54] is 122 pages and would require considerable training for an organisation's staff to be able to deliver a website substantially compliant with it. I do note here that compliance with this is required by the Information Security Manual published by the Australian Cyber Security Centre.

There is plenty of good guidance material available; so it will be a matter of mandating appropriate controls that are sufficiently specific. These should be minimum controls; and organisations should be required to do their own risk assessment and determine what is appropriate.

Mandating the equivalent of the PSPF and ISM, even for the lower security value information likely to be held in such platforms may result in appropriate security however would require significant engagement with Industry to garner support.

Protection from Harm

Protection from harm requires more than just technical security controls; accidental disclosures are common (e.g. use of 'cc' rather than 'bcc' when sending emails) or insider attacks[55].

It is also important to consider what harms need to be protected, many organisations would take the view that 'no one died, so what's the fuss ?'.

In developing the code, the OAIC needs to consider the relevant harms for services to children (and ideally would do so for the public).

Historically the courts have been unwilling to compensate the public for the inconvenience of having to replace documents; despite the document issuing organisations (e.g. credit card companies) being able to recover their costs. I would suggest that this needs to change,

---

[53] 'Penalty Notice (Re British Airways)' [3.25] <https://archive.org/details/ba-penalty-20201016>.
[54] 'OWASP Application Security Verification Standard (Version 5.0.0)' <https://github.com/OWASP/ASVS/raw/v5.0.0/5.0/OWASP_Application_Security_Verification_Standard_5.0.0_en.pdf>.
[55] 'Unauthorised Access to Client Information Held in the CRISSP Database' <https://ovic.vic.gov.au/wp-content/uploads/2021/03/Unauthorised-access-to-client-information-held-in-the-CRISSP-database.pdf>.

particularly where organisations have failed to implement even the minimal controls (including management controls to prevent ‘accidents’).

Responses to Specific Questions

1. Scope of Services covered by the Code

1.1 Are there additional APP entities, or a class of entities, that should be covered by the Code? Please provide reasons or evidence to support your view.

- As many health service providers provide services to children, 'health service providers' should not be automatically excluded. Health service providers and health records should be considered very carefully as creating a 'health record' is trivial e.g. "Fred is allergic to nuts".
- I would recommend that such providers are described in a manner with examples; a failure to provide examples has seen the Privacy Act in Australia deliver only a fraction of it's potential.
- The Code should also apply to Government agencies that provide services to children, as children deserve the same protection regardless of who is providing the service and additionally, many Government agencies are effectively monopolies where there is no choice but to use the Government's service.

1.2 No.

1.3 A criteria along the lines of 'likely to be accessed by children' should be sufficient.

- What we have seen, is 'gaming' of the legislation by claims that it's not about you, it's about your device, we can't identify you, even though we assign you a numeric identifier. This gaming appears to play on the mis-interpretation of information privacy as a breach of confidence action in Equity.

2. When and how the Code should apply to APP entities

2.1 Likely to be accessed by children, should be assessed on the basis that it is likely a child will have access to this service. It should be written in such a way that the service has to show why it is unlikely that a child would access the service.

2.2 No response.

2.3 An indicative, but non-exhaustive criteria should be provided, however the courts should also be allowed to extend the criteria to avoid 'gaming' of the criteria.

2.4 Age gating would be more relevant to services that require the user to authenticate to the service.

2.5 No response.

2.6 Personal information covered by other laws e.g. surveillance device laws should have different requirements. This would include where the information is covered by legislative secrecy provisions and/or 'personal affairs' considerations. Use of public transport[56] is another category of information that should attract additional protections.

2.7 Risk management, according to International Standards, like AS/NZS ISO 31000, deals with the harm that is likely and reducing the harms to acceptable levels. Where vulnerable children are involved (e.g. A parent has a AVO against another parent), serious harm can arise from simply disclosing the child's name and address. The code should focus on the risk of harm

[56] *Transport (Compliance and Miscellanous) Act 1983 (Vic)* s221.

to the child; and require APP entities to adequately address this; a key problem with this is that protecting their customers is yet taken seriously by APP entities as a need.

The data breaches that occur due to basic issues not being addressed is clear evidence that protecting customer's personal information is not given the attention it deserves. A key factor in this is the Moral Hazard[57] that arises as APP Entities do not bear the impact on their failures.

3. Age range-specific guidance

3.1 No Response

3.2 No Response

3.3 No Response

4. APP 1 – open and transparent management of personal information

4.1 The usual approach is layer communication methods with sections specific to audiences, e.g. the child and the child's parent's. Such methods should include 'plain english' versions requiring no more than 6th grade English for adults.

4.2 Yes – APP entities should ensure that obligations are met for all relevant segments of their user base. It should also apply to a service offered to parents that enables them to manage their child e.g. a Health Practice, if a child wants to know how the health practice will manage their personal information, the child should be able to access material to do so.

4.3 Internal procedures need to be shown to be effective, many organisations internal procedures are incomplete, dysfunctional and see stakeholders over looked.

4.4 The biggest change requires for APP entities to recognise the rights of the people that they collect information from, currently this is a game of 'smoke and mirrors', as illustrated by the 'about the device' defence.

4.5 APP1 with regards to Privacy Statements and Collection Notices, should be applied as a legal agreement, people are agreeing to provide you with their personal information in exchange for a service. Most 'privacy statements' or 'collection notices' are written as marketing documents to entice people to use the service or that everything is 'fine' and that it is risk free. There is also passing off of responsibilities to third party providers engaged by the lead entity in a manner that is not appropriate; as the lead entity – you are and should be held accountable for 3rd party providers that you engage.

[57] 'Moral Hazard' <https://en.wikipedia.org/wiki/Moral_hazard>.

5. APP 2 – anonymity and pseudonymity

5.1 Firstly, for services to be anonymous, the they must not use information provided in the provision of the service to the child. This includes not using ip addresses and online monitoring tools that track user usage of a website (typically in conjunction with a cookie based identifier or pseudonym). Where pseudonyms (or 'nick names') are used, then the meaning of these words must be as understood in plain English not the current legal 'double speak'[58] where we don't know who you are because we don't know your name but we identify you as customer 1001.

5.2 It depends on what you mean by 'identify'; if you mean login with a username and password (or equivalent) then the child has identified themselves. If you mean supply additional information, such as a email address to confirm their account then additional verification data should be minimised; noting that steps should also be taken to prevent adults from pretending to be children for nefarious purposes.

5.3 Age assurance technologies provide some information about you as a web site visitor, so you are no longer truly anonymous at that point – even for a particular 'session' the system knows you meet age criteria.

5.4 No further response.

6. APP 3 - collection of solicited personal information

6.1 I would apply a very high bar to any 'reasonably necessary' test, far closely to strictly necessary. APP entity's should be able to show and justify every field or attribute they collect about a child.

6.2 Children generally have a concept of 'fair' – open, transparent, honest, respecting others rights. The 'lawful' aspect of this is far harder to describe, because laws and the context of their application to digital systems is in it's infancy; a child is hardly going to known that section 247G of the Crime Act in Victoria may make it unlawful to access information on the child's device.

6.3 Current practices, with the use of covert tracking technology are likely to be considered unfair. The Hon Victor Perton, noted the following in the parliamentary debates of the Surveillance Devices Bill in Victoria in 1999:

> "The importance of such privacy issues is growing. If members of the public were aware of the data being collected every time an American Express card, Mastercard or Fly Buys card is used they would realise the extraordinary trail being left. Data relating to someone's shopping bag probably does not mean much, but when it is used with modern data warehousing and analytical tools, the most extraordinary and accurate profiles can be created, whether for the shadow Attorney-General, the honourable member for Northcote, the Parliamentary Secretary, the Clerk or the Hansard reporter.
>
> People are running large business ventures, selling and analysing personal data and using it in an endeavour to manipulate others, whether for the purposes of inducing shopping patterns or for other reasons."

[58] 'Double Speak' <https://en.wikipedia.org/wiki/Doublespeak>.

We can see the harm from such profiling and the level of awareness of adults on how to deal with in articles, such as the article titled “After my miscarriage, ‘big data’ kept haunting me”[59]. Image if this were a confused teenager who has discovered that she is pregnant and has a mis-carriage or otherwise sees the pregnancy end.

6.4 Genuine consent from children would be problematic because they are not of the age of consent, such consent should be provided by their parents or guardians.

6.5 No response provided.

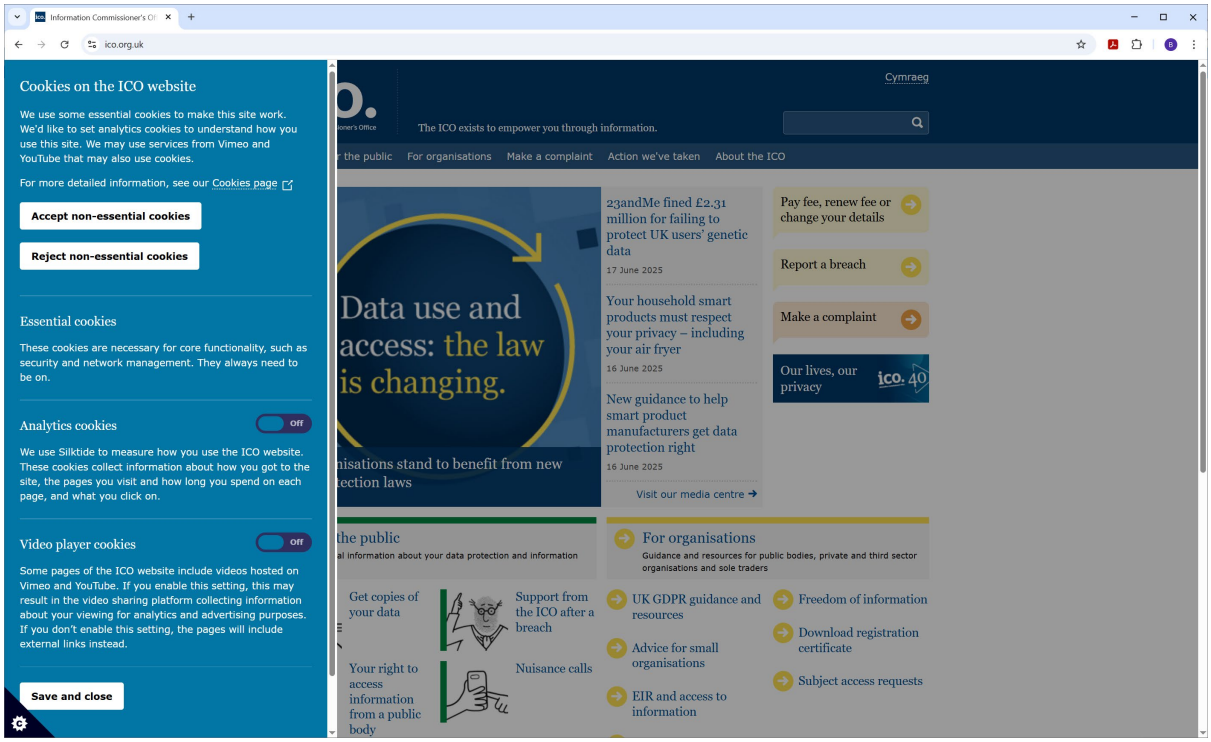
7. APP 4 – dealing with unsolicited personal information

7.1 If this personal information is not relevant to their business, it should be discarded. If it is necessary, the consent for it’s use should be sought and such use must be beneficial to the child.

7.2 No further response provided.

8. APP 5 – notification of the collection of personal information

8.1 The UK ICO’s website has a reasonable example of a privacy consent widget that doesn’t overly detract (or interfere with privacy of attention) from their website. (See below). The widget is accessed by clicking on the C inside a start at the bottom left corner of the screen.



The content of the notice should follow the same criteria as privacy policies to make sure if it accessible.

[59] ‘After My Miscarriage, “big Data” Kept Haunting Me’ <https://www.smh.com.au/lifestyle/life-and-relationships/reams-of-data-are-gathered-about-us-during-our-most-private-moments-20190618-p51z1d.html>.

8.2. Options include the provision of notifications in a range of languages, and supporting accessibility aids (that are privacy friendly).

8.3 Not requiring consent, in this context is not appropriate. Circumstances where consent isn't required are for circumstances where there is no expectation of privacy - photograph people in a public place and not wanting to create absurd situations where a person appearing in the background of a family happy snap creates an issue. I note here that publication of a family happy snap in a magazine for profit creates additional legal considerations.

As this context requires express or implied consent, I would say no that such circumstances do not exist, beyond any permitted by law – e.g. a child at risk of harming themselves or others. I should not here that most APP use and disclosure exemptions do not relate to collection. A child visiting a website on sensitive health topics should not necessarily see a disclosure to child protective services or the police.

8.4. No further response provided.

9. APP 6 – use or disclosure of personal information

9.1 No further response beyond the responses already provided.

9.2 APP entities must ensure that contracts for zero cost services, do not allow for the information to be reused for secondary purposes that are not consented to, this would require the APP entities to read contracts and not use certain zero cost services.

9.3 No response provided.

9.4 'reasonably expected' secondary uses should be interpreted narrowly.

10. APP 7 – direct marketing

10.1 For children, I don't think it is appropriate for their information to be used for the purposes of direct marketing.

10.2 APP entities should require opt-in, and then provide a choice of opting out later. APP entities must be required to ensure such mechanisms are in place.

10.3 See 10.1, APP entities should not use children's information for direct marketing or if they do, they should be restricted from certain categories where marketing to children is not appropriate (e.g. Alchol, Gambling, etc.).

11. APP 8 – cross-border disclosure of personal information

11.1 APP entities would need to have a far better understanding of how web applications work than most of them currently do. 'Cloud' delivered services make this particularly difficult, as they are delivered from any where in the globe and using support staff also from any where in the globe. Unless APP entities host their own systems and support them with local staff, it is virtually impossible to provide any assurance over cross-border disclosures to the US and China. While we Australian values and politics may not be aligned to China, China and other countries underpin the delivery of cloud services.

11.2 APP entities should advise children and parents of the risks of cross-border data transfers. This is particularly problematic for people living in Australia, who have family in countries that have different values and political values to Australia.

11.3 No further response.

12. APP 10 – quality of personal information

12.1 Given a child's evolving development and digital engagement stages, 'up-to-date' or 'relevant' is far more dynamic with children; and children are also more inclined to make mistakes as they learn leading to less 'accurate' information.

12.2 APP entities should provide greater effort in verifying that personal information collected is intended and not a mistake; additionally, it should be used for a shorter period of time as children's lives are more 'dynamic'. This would require additional effort to determine appropriate checks and put 'use by dates' on the date and respect those use by dates.

12.3 APP 10 should be applied more strongly with reference to children.

13. APP 11 – security of personal information

13.1 APP entities should be required to comply with an objective standard, like the Australian Government's Protective Security Policy Framework and Information Security Manual and this needs to be a wholistic in it's nature. Standards like ISO27001/2, that only provide guidance, lack the rigour suitable for the current online environment which is more like a war zone than the quiet streets in our relatively green leafy suburbs.

13.2 APP entities should be required to comply with an objective standard, like the Australian Government's Protective Security Policy Framework and ISM for organisational measures. Child safety laws should be considered and personnel screening requirements like a 'Working With Children Check' should be required.

13.3 APP entities should be given objective guidance in the Privacy Code, unless there is other specific legislative requirements relevant to their business. APP entities should be required to provide reports on de-identification of data and/or deletion of data; noting that many online systems retain information for ever, with mandatory reporting to senior executives, audit and risk committees and similar.

13.4 No further comments.

14. APP 12 – access to personal information

14.1 Students should be given access to online portals, so that they can access their own personal information, subject to restrictions.

14.2 Most of the circumstances are described in APP 12.3 a,b,d,e,f,g,h,I.

14.3 Where a parent or guardian has custody of the child, with no restrictions, they should be able to make an access request on behalf of their child and receive a copy of their child's personal information. Ideally the child would consent to this; however there should be provision for a parent or guardian to request this information provided that there are no restrictions on that parent (e.g. some form of restraining order).

14.4 Ideally, these should be 'self-help' and 'automated' so less than 24 hours. Relying upon manual request processes via Privacy Officers shows an organisation's practices have not kept pace.

14.5 The format should be human readable to the extent possible, and readily searchable. APP entities should not be allowed to provide "Binary" or machine only readable information that is not intelligible to the Parent / Child.

14.6 Nothing further than the above.

15. APP 13 – correction of personal information

15.1 See 12.1.

15.2 Via the online portals mentioned in 14.1, children should be able to correct information about themselves.

15.3 See 14.3.

15.4 See 14.4.

15.5 Care needs to be taken here with adult topics (drugs, alcohol, gambling). The harm that can occur to children is illustrated by the article "After my miscarriage, 'big data' kept haunting me"[60]. The article illustrates the author's sense of powerlessness to inform 'big data' that she was no longer pregnant and didn't want to see these ads and didn't know how to do anything about it because of a lack of understanding of how the technology worked. Children need to be provided with readily accessible portals to be able to correct information about themselves, so that they are not 'haunted' by changing circumstances.

[60] Ibid.