



**Association for data-driven
marketing & advertising**

CHILDREN'S ONLINE PRIVACY CODE ISSUES PAPER

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER

01 AUGUST 2025



Level 27
100 Barangaroo Road
Sydney, NSW, 2000
ABN: 53 156 305 487

01 August 2025

Office of the Australian Information Commissioner

GPO Box 5288, Sydney NSW 2001

By email: copc@oaic.gov.au

Dear Privacy Commissioner

The **Association for Data-driven Marketing and Advertising (ADMA)** is the principal industry body for data-driven marketing and advertising, and the ultimate authority and go-to resource for effective and creative data-driven marketing across all channels and platforms, providing insight, ideas and innovation for today's marketing industry.

ADMA welcomes the opportunity to make a submission to the Office of the Australian Information Commissioner in relation to the Children's Online Privacy Code Issues Paper.

If you have any questions about our submission, please do not hesitate to contact me [REDACTED] for further discussion.

Regards

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1. Executive summary

The Office of the Australian Information Commissioner (**OAIC**) is seeking feedback from relevant stakeholders, via the Children's Online Privacy Code Issues Paper (**Issues Paper**), into the development of the Children's Online Privacy Code (**the Code**).

The Code, which is mandated by the *Privacy and Other Legislation Amendment Act 2024*, seeks to enhance privacy protections for children in the digital world by ensuring that their personal information is protected when engaging online, through strengthened privacy protections.

Representing over 600 brands, the Association for Data-driven Marketing and Advertising (**ADMA**) is the largest marketing and advertising association in Australia, and the principal industry body for data-driven marketing and advertising. As an industry association, ADMA is the ultimate authority and go-to resource for effective and creative data-driven marketing across all channels and platforms, playing an important role in helping our members adhere to new obligations in a way that can be operationalised and is consistent with industry best practice.

In our capacity representing the data-driven marketing industry, ADMA's submission to the OAIC's consultation on the development of the Code focuses mostly on marketing directed at children, with a view on the scope of services intended to be covered by the Code.

Marketing directed at children

Of particular focus for digital marketers is how the Code should be applied, or complied with, in relation to marketing directed at children.

As the principal industry body for data-driven marketing and advertising, and the ultimate authority and go-to resource for effective and creative data-driven marketing across all channels and platforms, ADMA maintains that by introducing proportionate reforms to the *Privacy Act 1988* (Cth) (**Privacy Act**), the OAIC can achieve its objective of protecting children when engaging online, without needing to further amend APP 7 obligations with respect to marketing practices directed at children.

In our submission, ADMA argues that the Australian digital marketing industry is beset with legislative complexity, for the reasons outlined in [Section 6](#). In [Section 7](#), we explain why uncertainty as to the possible implementation form of the tranche 2 Privacy Act reforms, particularly in relation to 'agreed-in-principle' proposals on direct marketing, compounds an already complex regulatory ecosystem that digital marketers need to navigate. The collective impact of legislative complexity as applied to digital marketing practices, coupled with uncertainty on further Privacy Act reforms, are cause for circumspection towards proposals that consider introducing additional, or changed, obligations on marketing practices directed at children.

The Children's Code-related Privacy Act provisions introduced by the *Privacy and Other Legislation Amendment Act 2024* focus upon *services*, not digital marketing conducted outside of *provision* of a *service* likely to be accessed by children, where those services are *likely to be accessed by children*. This is an appropriate scope for focus of the Code: the Code is intended to protect children in relation to services that they are likely to access, and not to anticipate future regulation as to direct marketing or targeting outside of those services. However, this does not mean that digital marketing outside of provision of services likely to be accessed by children is under-regulated, or that tranche 2 Privacy Act reforms should not include proportionate regulation of digital marketing manifestly directed towards children or other vulnerable audience segments. ADMA states in this submission, as ADMA has stated in other submissions, ADMA's support for proportionate and balanced expansion of coverage of the Privacy Act provisions that address digital marketing, where coupled with clarification and simplification of the statement of the relevant rules and how they operate together with overlapping provisions of other statutes.

Scope of services covered by the Code

In relation to the scope of services to be covered by the Code, ADMA submits that the application of the Code should be very clearly defined, including being accompanied by unambiguous guidance that can be easily understood by all stakeholders. The concept of '*likely to be accessed by children*' should reference the part of the service which manifestly is attractive to children, which is directed at or focused for children. The Code should not apply to other aspects of a service or other activities of regulated entities, which might be accessed by children. This is the subject of [Section 9](#) of our submission.

2. Consumer trust is a bedrock of the digital marketing ecosystem

Brand trustworthiness is a cornerstone of building and maintaining consumer trust in the digital marketing ecosystem. The data-driven marketing and advertising industry's livelihood and reputation depend on protecting consumers' privacy.

ADMA recognises that good privacy practice is the right thing to do, in addition to a compliance obligation. And good privacy practice is crucial when considering the best interest of a child using or accessing online services. Good privacy law should not place the burden on individual Australians, particularly not children, to detect and deter abuses and possible privacy harms.

3. Children's Online Privacy Code

The Code, which is mandated by the *Privacy and Other Legislation Amendment Act 2024*, seeks to enhance privacy protections for children in the digital world by ensuring that their personal information is protected when engaging online, through strengthened privacy protections.

The Code will apply to APP entities¹ if they provide a social media service, a relevant electronic service or a designated internet service,² where the service is likely to be accessed by a child, and is not a health service.³ Additional inclusions or carveouts may be applied to the scope of APP entities or class of entities bound by the provisions of the Code.

The Code will specify how regulated services must comply with the Australian Privacy Principles (**APPs**) of the Privacy Act in relation to children's personal information, and may impose additional requirements provided they are not contrary to, or inconsistent with, existing APPs. As noted in the Issues Paper, the Code presents a significant opportunity to elevate the privacy practices of entities, that will benefit Australians more broadly, particularly for individuals within the wider community who are at higher risk of harm due to vulnerability factors associated with, for example, low levels of literacy or education, or who live with impaired cognitive functions.

Through the Issues Paper, the OAIC seeks feedback from stakeholders on several matters being considered for the Code, including matters related to APP 7 direct marketing. Direct marketing involves the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services.⁴ Existing provisions under APP 7 of the Privacy Act provide that an APP entity must not use or disclose personal information it holds for the purpose of direct marketing, unless a valid exception applies. The Issues Paper poses questions for stakeholders to consider how APP 7 should be applied, or complied with, in relation to the privacy of children.

¹ As defined in s6(1) of the Privacy Act.

² The terms 'social media service', 'relevant electronic service' and 'designated internet service' have the meaning provided in s13, s13A and s14 respectively of the *Online Safety Act 2021*.

³ As defined in s6(1) of the Privacy Act.

⁴ Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, p 81.

4. Legislative complexity and privacy reform uncertainty

The Australian digital marketing industry is beset with legislative complexity, for the reasons outlined in [Section 6](#) below.

Uncertainty around tranche 2 Privacy Act reforms – if, when, what – particularly in relation to ‘agreed-in-principle’ proposals on direct marketing, targeting and trading, compounds an already complex regulatory ecosystem that digital marketers are forced to navigate. We discuss this topic further in [Section 7](#) below.

This uncertainty is intensified by government-driven discussions on Australia’s productivity challenges,⁵ and initiatives seeking to drive business efficiencies and boost productivity – such as those proposed under **Pillar 3, Harnessing data and digital technology** of the Government’s five pillar productivity growth agenda.⁶

5. ADMA’s view on marketing directed at children

The existing legislative complexity inherent in digital marketing practices, coupled with uncertainty on further Privacy Act reforms, fosters ADMA’s circumspection towards proposals that consider introducing additional, or changed, obligations on marketing practices directed at children.

Additional obligations on marketing directed at children, if introduced by the Code, risk becoming a potential overreach when used to regulate all forms of direct marketing that may or may not be to a child audience.

As per our submission to the Privacy Act Review – Discussion Paper,⁷ and the Productivity Commission Pillar 3 review,⁸ ADMA is committed to the introduction of proportionate legislative reforms to the Privacy Act.

⁵ Australian labour productivity declined by -0.1% in 2024’s fourth quarter, and by -1.2% for 2024 as a whole. Productivity Commission. *Quarterly productivity bulletin – March 2025*, <https://www.pc.gov.au/ongoing/productivity-insights/bulletins/quarterly-bulletin-march-2025/bulletin-march-2025.pdf>. See also: in the five years preceding the pandemic, productivity growth was stagnant, while for the decade up to 2019, it was the slowest in 60 years. Productivity Commission, 2024. *Creating a more dynamic and resilient economy, Terms of Reference*, <https://www.pc.gov.au/inquiries/current/resilient-economy/terms-of-reference>

⁶ Productivity Commission, 2024. *Creating a more dynamic and resilient economy, Terms of Reference*, <https://www.pc.gov.au/inquiries/current/resilient-economy/terms-of-reference>

⁷ Available at https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/published_select_respondent

⁸ Productivity Commission. *Responses to Pillar 3: Harnessing data and digital technology*, <https://engage.pc.gov.au/projects/data-digital/page/pillar-3-responses>

Section 8 of our submission outlines what ADMA considers as proportionate reforms to the Privacy Act, including:

1. introducing an overarching, but structured and balanced, test of reasonableness to personal information handling, supplemented by clear, unambiguous guidance;
2. adopting an outcomes-based framework; and
3. implementing a staged removal of the small business exemption.

ADMA submits that by introducing proportionate reforms to the Privacy Act, the OAIC can achieve its objective of protecting children in particular, but vulnerable Australians more broadly, when engaging online, without needing to amend APP 7 obligations with respect to marketing practices directed at children.

The rest of this submission provides justification for ADMA's position on why the Code need not introduce additional APP 7 obligations when considering marketing directed at children.

Should the Code be amended to introduce new or changed APP 7 obligations for marketing practices directed at children, then ADMA would welcome the opportunity to discuss practical considerations to be implemented into the Code – noting that processes currently exist under the SPAM Act and in relation to APP 7 of the Privacy Act with regards to consent and unsubscribe facilities. ADMA members already offer many ways for customers to opt-out of direct marketing.

6. Legislative complexity in digital marketing

Each Australian organisation engaged in digital marketing – most Australian businesses other than small businesses – must navigate legislative complexity, in part attributable to the following factors:

- Factor 1 - Complex digital marketing legislative ecosystem.
- Factor 2 - Cost of legislative reforms.
- Factor 3 - Overreliance on consent models.
- Factor 4 - Outdated legislation in the digital age.

The four factors are expanded upon, next.

6.1. Factor 1 - Complex digital marketing legislative ecosystem

A complex digital marketing ecosystem is caused by:

A plethora of legislation: Data-driven marketing practices are subject to a surfeit of legislative obligations, including those imposed under the Privacy Act, the *Spam Act 2003 (Spam Act)*, Australian Consumer Law and other protections under the *Competition and Consumer Act 2010 (Cth)* and the *Competition and Consumer (Consumer Data Right) Rules 2020 (Cth)*, *Telecommunications (Telemarketing and Research Calls) Standards 2017 (TIS)* under the *Telecommunications Act 1997*, *Do Not Call Register Act 2006 (DNCR Act)*, the *Online Safety Act 2021*, and state-based trade promotions legislation.

Introducing more obligations for marketing practices, when marketing is directed at children, to an already complex digital marketing regime, will increase direct and indirect compliance costs and enforcement regime burdens for regulated entities.

Complexity through additional layers of local and international obligations. Legislative complexity is compounded for (1) entities bound by sector-specific legislation,⁹ (2) those that are Australian Competition and Consumer Commission (**ACCC**)-accredited data holders or data recipients with obligations under the Consumer Data Right, and (3) those regulated by other jurisdictions, including European Union (**EU**) legislation where the web of regulatory compliance obligations imposed by the General Data Protection Regulation (**GDPR**), Digital Services Act, Digital Markets Act, Data Act, Network and Information Systems Directive 2 and the EU Artificial Intelligence Act encapsulates the developing state of broader digital governance. For these entities, significant time, money and effort are expended in assessing compliance of new digital marketing campaigns, with an expectation that expenditure will escalate should the Code introduce additional obligations for direct marketing practices directed at children.

Figure 1, for example, visualises the wave of digital regulation introduced in the EU over the past ten years, as an example of legislative complexity *in extremis*.

⁹ Examples of industry-specific protections include prudential regulation for APRA-regulated entities, the Telecommunications Consumer Protections Code (**TCP Code**) which protects customers who use mobile phones, landlines and internet services, *Australian Securities and Investments Commission Act 2001 (Cth)* for financial services, and National Energy Customer Framework for the energy sector, among others.

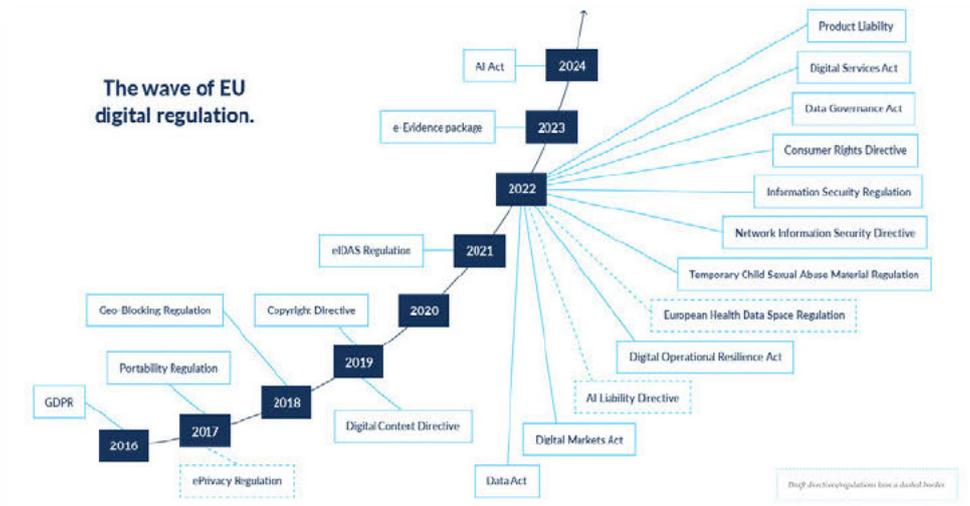


Figure 1 Wave of EU digital regulation¹⁰

Contradictions within and among legislation: Disparate, sometimes conflicting, legislative obligations and regulatory carveouts exist. For example: APP 7.8 of the Privacy Act provides that where an act or practice of an APP entity is subject to the Spam Act, the DNCR Act, Division 5 of Part 7B of the *Interactive Gambling Act 2001*, or other legislation prescribed under the regulations, then APP 7 does not apply to the extent that the legislation applies. If an organisation that is an APP entity is exempt, wholly or partially, from the Spam Act, the DNCR Act, Division 5 of Part 7B of the *Interactive Gambling Act 2001*, or other legislation prescribed under the regulations, then APP 7 still applies to the acts and practices of that organisation to the extent of that exemption.

Any amendment to APP 7 provisions introduced by the Code, to marketing practices directed at children, will need to negotiate existing APP 7 carveouts referencing other marketing legislative regimes.

Evolving digital environment: The Privacy Act and the Spam Act are two key legislative instruments that govern data practices and data-driven marketing. Both were designed to be platform-agnostic, allowing them to be applied as new channels emerged over time. However, the digital environment has evolved in such a way that the intersection of these Acts is no longer clear. For example, the definition of 'electronic message,' which is meant to clarify when the Spam Act applies, has become increasingly ambiguous in a digital-first economy. While reform is expected to provide much-needed clarity, the current lack of precision impacts productivity in regulatory applications, particularly as businesses need to find the right balance between legalistic and sensible interpretation.

Scope ambiguity will exacerbate if new APP 7 obligations are introduced by the Code, applying to marketing practices directed at children, without any definition clarification promised by Privacy Act reforms.

¹⁰ iapp. iapp Organizational Digital Governance Report 2024
https://iapp.org/media/pdf/resource_center/organizational_digital_governance_report.pdf

6.2. Factor 2 - Cost of legislative reforms

The introduction of additional obligations, such as introducing new APP 7 requirements under the Code for marketing directed at children, overlaid with costs associated with complying with existing regulation, has created a complex matrix of obligations and risks for digital marketers. As legislative scope expands, so do the costs for both regulated entities and Regulators.

6.3. Factor 3 - Overreliance on consent models

From a survey of young people, conducted by Reset.Tech Australia,¹¹ the findings show that children expressed the need for explicit consent before data collection, sharing, or use, emphasising that meaningful consent is often lacking in their online experience.

ADMA submits that, in today's digital economy, an overreliance on consent-based frameworks introduces added complexity to data-driven marketing practices. While consent is a requisite obligation to the operation of several principles of the Privacy Act,¹² and consent provides the authorisation for businesses to send commercial electronic messages to consumers under the Spam Act, consent is a more appropriate and effective mechanism when used in a narrow range of situations where individuals most need to proactively exert control over their personal information. Too many requests for consent may lead to consent fatigue- which, in turn, devalues consent. An ability to provide, or withdraw, one's consent is no longer practical for consumers, nor easily implementable for businesses. In seeking consent, companies risk driving unintended consumer harms, in the form of consumer frustration or consent fatigue.

Despite views expressed by young people in the Reset.Tech Australia survey, there can be no expectation that consent terms (along with privacy policies, collection notices and terms and online terms and conditions) will be read by the average consumer, let alone the average child.

6.4. Factor 4 - Outdated legislation in the digital age

The need for Australian laws to keep pace with evolving digital markets is a concern shared by Government, Regulators, business and industry groups, and Australian consumers.

The Privacy Act Review Report 2022¹³ considered whether *'the Privacy Act and its enforcement mechanisms remain fit for purpose in an environment where Australians now live much of their lives online and their information is collected and used for a myriad of purposes in the digital economy'*. As the then Attorney-General, the Hon Mark Dreyfus KC, noted in the second reading speech introducing the *Privacy and Other Legislation Amendment Bill 2024* (Cth):

¹¹ Reset.Tech Australia, Consultation with young people about the Children's Online Privacy Code; especially Transparency, Geolocation, Advertising & EdTech, page 11.

¹² Consent is both an exception to a general prohibition against personal information being handled in a particular way (e.g., APP 6.1(a)) or an authorisation to handle personal information in a particular way (e.g., APP 7.3 and APP 7.4).

¹³ Attorney-General's Department. Privacy Act Review Report 2022, https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf

“Evolutions in technology and the way people use it continue to vex those who share information online, and those charged with regulating it. It is essential that Australians are protected by a legal framework that is flexible and agile enough to adapt to changes in the world around them. The Privacy Act has not kept pace with the adoption of digital technologies.” (Hon Mark Dreyfus KC)¹⁴

This concern is echoed in the Issues Paper, which provides that “(e)xisting privacy laws have not kept pace with these changes in digital engagement or the scale of data collection.”¹⁵

The fact that legislation has not kept up with a rapidly changing data-driven ecosystem has contributed to complexities for Government, Regulators and regulated entities, and has increased the potential for serious harms to consumers.

Adding more obligations for marketing directed at children, without addressing reforms that will modernise Australia’s privacy framework, will further exacerbate problems associated with a Privacy Act that is out of date and unfit for purpose in today’s digital economy.

6.5. Accumulative effect of legislative complexity

Four factors result in legislative complexity for entities’ digital marketing practices – [1] a complex digital marketing legislative ecosystem; [2] increased compliance costs and enforcement regimes associated with expanding legislative scope; [3] an overreliance on consent models; and [4] legislation out of step with the rapidly evolving digital age.

The consequences of this legislative complexity are:

- Significant time, money and effort expenditure associated with assessing whether new digital marketing campaigns can proceed, compliantly.
- Entities that have neither the financial means or in-house resources to navigate legal complexity adopt a risk-averse approach when considering new campaigns or marketing initiatives. The net result is that many entities are disadvantaged when competing against well-resourced competitors.
- Stifled innovation, where novel digital advertising opportunities are scuppered, in favour of more traditional, ‘safer’, practices.
- Compliance breaches, when companies apply their own interpretation to opaque obligations.

¹⁴ Mark Dreyfus MP, 12 September 2024. Privacy And Other Legislation Amendment Bill, <https://www.markdreyfus.com/media/speeches/privacy-and-other-legislation-amendment-bill-markdreyfus-kc-mp/>

¹⁵ Office of the Australian Information Commissioner. Children’s Online Privacy Code Issues Paper, <https://www.oaic.gov.au/engage-with-us/consultations/childrens-online-privacy-code-consultation-for-industry,-civil-society,-academia-and-other-interested-stakeholders>

- Reduced competition, where legislative complexity can be prohibitive - particularly for small and medium-sized enterprises (**SMEs**),¹⁶ with limited or no access to in-house legal counsel, or no ability to afford external counsel fees – and also a barrier to the ability to compete with larger corporations.
- Uncertainty for consumers in knowing their rights under different consumer protection and privacy laws, or how to access help, lodge a complaint or seek redress, erodes consumer confidence in the market.

For regulated entities, the risk associated with financial penalties, being ordered to change business practices or reputational harm resulting from noncompliance, is forcing decisions on whether and how organisations categorise, prioritise and respond to digital governance.

As we presented in our submission to the Productivity Commission Pillar 3 review,¹⁷ legislative complexity negatively impacts productivity, particularly for regulated entities motivated to (1) do the right thing, (2) comply with legislative obligations, (3) avoid compliance breaches, (4) preserve brand reputation, and (5) maintain consumer trust.

7. Uncertainty on timelines and scope of Privacy Act reforms

At the time of development of this Code, it is unclear as to whether, when and in what form tranche 2 Privacy Act reforms will proceed, and in particular ‘agreed-in-principle’ proposals on direct marketing, targeting and trading.¹⁸

Any new rules creating additional obligations as to digital marketing directed at children should take into account further changes forming part of tranche 2 Privacy Act reforms.

The Children’s Code-related Privacy Act provisions introduced by the *Privacy and Other Legislation Amendment Act 2024* focus upon *services*, not digital marketing conducted outside of *provision* of a *service* likely to be accessed by children), where those services are *likely to be accessed by children*. This is an appropriate scope for focus of the Code: the Code is intended to protect children in relation to services that they are likely to access, and not to anticipate future regulation as to direct marketing or targeting outside of those services. This does not mean that digital marketing outside of provision of services likely to be accessed by children is under-regulated, or that tranche 2 Privacy Act reforms should not include proportionate regulation of digital marketing manifestly directed towards children or other vulnerable audience segments. ADMA’s training materials for digital marketers specifically address responsibilities of digital

¹⁶ Using the Australian Bureau of Statistics definitions: Businesses employing 0-19 people are classified as small businesses, those employing 20-199 people are classified as medium sized and those employing more than 200 people are classified as large businesses.

<https://www.abs.gov.au/ausstats/abs@.nsf/Previousproducts/8155.0Main%20Features42016-17?opendocument&tabname=Summary&prodno=8155.0&issue=2016-17&num=&view=>

¹⁷ Productivity Commission. *Responses to Pillar 3: Harnessing data and digital technology*,

<https://engage.pc.gov.au/projects/data-digital/page/pillar-3-responses>

¹⁸ Refer Proposals 20.1, 20.2, 20.4, 20.5, 20.6, 20.7, 20.8, 20.9. Australian Government. *Government Response Privacy Act Review Report*, <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>

marketers in content and addressability of marketing communications that are directed towards children, or likely to be seen by children. These responsibilities include assessing risk of harm and appropriateness of the communication to the recipient's best interests.

Proportionate reforms introduced to the Privacy Act can address marketing practices in particular, and uses or disclosures more broadly, of personal information handling related to vulnerable individuals, which includes children. By introducing proportionate privacy reforms, ADMA submits that the Code need not go further in regulating marketing directed at children.

We outline what proportionate legislative reforms looks like, next.

8. Legislative proportionality in Privacy Act reforms

Three elements form the basis of ADMA's view on legislative proportionality applied to Privacy Act reforms:

1. Introduction of an overarching, but structured and balanced, test of reasonableness for personal information handling.
2. Adoption of an outcomes-based framework.
3. Implementation of a staged removal of the small business exemption.

By introducing these elements, ADMA submits that such arrangements will allow the OAIC to achieve its objective of protecting children in particular, and vulnerable Australians more broadly, from harmful digital marketing practices, when they engage in the digital world.

We discuss each of the three elements in more detail, below.

8.1. Privacy Act reforms: Introduce an overarching test of reasonableness

To achieve legislative proportionality with tranche 2 Privacy Act reforms, ADMA proposes that the Government introduce an overarching, but structured and balanced, test of reasonableness to personal information handling, supplemented by clear, unambiguous guidance for regulated entities on how to meet the test and, equally, what would not meet the threshold.

As per our submission to the Privacy Act Review – Discussion Paper,¹⁹ ADMA believes that where a collection, use or disclosure of personal information is clearly and broadly harmful, the Privacy Act should prohibit that act or practice. It should not fall to the individual to identify and avoid, or mitigate, that harm.

¹⁹ Available at https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/published_select_respondent

Benefits realised through the introduction of an overarching test of reasonableness include:

- It will promote compliant practices, helping to build a more trustworthy digital economy.
- It will rule out the most exploitative data practices, providing a basis for trust, by shifting responsibility for avoiding harms on APP entities that cause those harms.
- For digital marketers, it will help protect consumers from ‘dark patterns’²⁰ which otherwise may nudge users towards consenting to more privacy-intrusive practices, or encourage them to choose more privacy-intrusive settings.
- It will address obligations currently covered under complementary legislative regimes, such as misleading or deceptive conduct, unconscionable conduct or unfair contract terms, covered in Parts 2-1, 2-2, and 2-3, respectively, of the *Competition and Consumer Act 2010* - Schedule 2 The Australian Consumer Law.
- It will alleviate the overreliance on consumer consent models, and reduce the likelihood of consent fatigue.
- It will help address other practices that have eroded consumer trust in digital marketing, such as profiling and online tracking.
- It will mitigate any imperative for more granular, technical and complex (to draft, implement and administer) reforms, such as those mooted to address data sharing, customer loyalty schemes,²¹ targeting individuals using their personal information,²² trading in individuals’ personal information,²³ and general data broker practices.
- It will lower the level of vigilance required to protect against everyday privacy harms, improving digital trust, while allowing entities the confidence to operate within appropriate bounds.

The introduction of such a test should be supported by clear, unambiguous guidance provided to entities, articulating how they can meet the test and, equally, what would not meet the threshold. The absence of such guidance could lead to ambiguity, further fuelling complexity. The guidance should list protected categories of personal information, to thereby ensure that the use of such information aligns with the legitimate interest of the entity *and* the expectations of the consumer. The challenge will be to consider the application of the threshold test, to ensure guidance is neither too restrictive nor too broad, keeping privacy protection at the core, while not negatively impacting competition or innovation.

²⁰ See further James Baumeister and others (University of South Australia), *Patterns in the Dark: Deceptive Practices in Online Interactions, including Landscape Assessment: Dark Patters*, A report to the Data Standards Chair, November 2024, available at <https://dsb.gov.au/sites/dsb.gov.au/files/2024-11/report-patterns-in-the-dark.pdf>. The International Consumer Protection and Enforcement Network *Dark Patterns in Subscription Services Sweep Public Report 02 July 2024* defines ‘dark patterns’ as ‘*practices commonly found in online user interfaces and steer, deceive, coerce, or manipulate consumers into making choices that often are not in their best interests*’.

https://www.oaic.gov.au/_data/assets/pdf_file/0018/232623/Public-Report-ICPEN-Dark-Patterns-Sweep.pdf. ADMA. *Dark Patterns Information Sheet*, <https://www.adma.com.au/resources/dark-patterns-information-sheet>

²¹ Refer Australian Competition and Consumer Commission recommendations included in https://www.accc.gov.au/system/files/2020/01/20201901/20201901_Customer%20Loyalty%20Schemes%20-%20Final%20Report%20-%20December%202019.PDF

²² Refer Proposals 20.1, 20.6, 20.8 and 20.9 on targeting to an individual using personal information, <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>

²³ Refer Proposals 20.1, 20.4 and 20.7 on trading personal information, <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>

8.2. Privacy Act reforms: Adopt an outcomes-based framework focusing on benefits and privacy harms

ADMA proposes that focus for privacy regulation more broadly, but Privacy Act tranche 2 reforms specifically, should be on those areas where outcomes are either a significant benefit to Australian consumers and the Australian economy, or avoid serious harms to individuals. We see this as striking the right balance between protecting the privacy of individuals and the interests of regulated entities in carrying out their functions or activities.²⁴

Several factors need to be considered, when assessing benefits or harms, to ensure the right balance of regulatory obligation is achieved. Consideration should be given to:

- The type and sensitivity of personal information.
- The vulnerability of the user cohort.
- The nature of processing activity.
- The risk of likely harm(s).
- The role of the entity in the processing arrangements, such as whether the entity is a controller or a processor.²⁵
- The type of entity processing personal information (e.g., processing of personal information when undertaken by a law enforcement agency versus a retailer).

ADMA submits that the level of legislative obligation be commensurate with the severity of risk, rather than a one-size-fits-all compliance regime that stifles innovation and suppresses productivity in low-risk environments.

Adopting legislative proportionality, where obligations are proportionate and outcomes-focused, would place greater responsibility and accountability on controllers engaged in high-risk practices, compared with smaller organisations with limited control over processing, or entities engaging in less risky personal information handling practices.

For SMEs and entities that are true processors, or that engage in low-risk privacy practices, adopting an outcomes-based approach, that balances benefits with harms, would reduce their compliance overhead, promote innovation, remove barriers for entry for SMEs, and increase competition. Holistically, these benefits would boost productivity.

By recalibrating legislation to focus on outcomes, Regulators can avoid excessive over-enforcement that does not materially address serious harms, thereby allowing them to focus on practices that promote consumer trust. This will give regulated entities more opportunities to uplift their data maturity more generally.

²⁴ s2A(1)(b), Privacy Act refers an object of the Privacy Act is to '*recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities*', <https://www.legislation.gov.au/C2004A03712/latest/text>

²⁵ The EU's GDPR recognises that not all organisations involved in the processing of personal data have an equal level of responsibility. The regulation includes distinct responsibilities for data controllers versus data processors. See GDPR. *GDPR data controllers and data processors*, <https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/>

8.3. Privacy Act reforms: Implement a staged removal of the small business exemption

To achieve legislative proportionality with privacy reforms, ADMA advocates for the removal of the small business exemption from the Privacy Act, but in a way that recognises SMEs' more limited capabilities. We support a staged, or staggered, removal of the exemption, along with the provisioning of significant resources and training to SMEs, to facilitate a smooth transition.

ADMA represents many SMEs that, through their membership engagement, commit to responsible and accountable best practice in digital marketing and advertising. Many SMEs have expressed a willingness to be held to the same standards for fair and responsible handling of personal information as currently apply to APP entities. The principal issue for many SMEs is not an unwillingness to implement good privacy practices, but rather their capabilities (technology systems, documentation of processes and practices, resources and knowhow) to implement compliance frameworks at a level required for APP entities. Obliging SMEs to meet the same obligations as large corporations, especially in low-risk privacy environments, may prove prohibitive for some SMEs, offer fewer opportunities for innovation, reduce their competitiveness and lower their productivity.

9. Scope of services covered by the Code

In relation to the scope of services covered by the Code, ADMA submits the application of the Code should be very clearly defined, including being accompanied by unambiguous guidance that can be easily understood by all stakeholders.

The concept of '*likely to be accessed by children*' should include the part of the service which manifestly holds itself out as attractive to children, which is directed at or focused to children. The Code should not apply to other things that regulated entities do, including discrete parts of a service which might merely be accessed by children. This distinction should be extrapolated to the types of online services regulated by the Code to prevent ambiguity in interpreting the scope of service covered by the Code.

ADMA notes further that the scope of regulated entities bound by the Code, for services "*likely to be accessed by children*" will include a broad range of entities – some already regulated, or some in which "*accessed by children*" element of their services is a much smaller part of their core business. Accordingly, compliance with the Code may (i) increase regulatory cost or burdens without a proportionate benefit to children, and/or (ii) result in some businesses removing the ability of children to participate at all. Given the importance of this element, it is our expectation that it is a key element of further consultation and discussion.