ADMA Association for data-driven marketing & advertising

1 Introduction

ADMA is the principal industry body for data-driven marketing and advertising in Australia. Data driven marketing collects, uses, discloses, and manages data that drives decision–making across a business. Data-driven marketing drives growth within a business, but equally if not responsibly planned and managed, can erode consumer trust and create substantial risk exposure for a business. For this reason, ADMA's community prioritises upskilling marketers in their compliance responsibilities. These teams are often at the frontline of a digital business, and both underpin and reflects a business' level of digital maturity.

2 Executive Summary

This short submission addresses some of the issues that have been raised by ADMA members in response to the Digital Platform Services Inquiry – March 2025 Final Report Issues paper (**Issues Paper**) published by the ACCC and in preparation for the significant changes that will flow from the Digital Platforms Services Inquiry over the coming years. The submission addresses the following key issues that are of importance to the data-driven marketing and advertising industry:

(a) Dark patterns
(b) Cookie deprecation
(c) Definitions that flow from the definitions in the Privacy Act amendments
(d) Adoption of privacy enhancing technologies (PETs)
(e) Growth in artificial intelligence
(f) International decisions on biometrics

The focus of this submission is on two topic areas:

(a) major developments and key trends in certain jurisdictions relating to digital platform services, and
(b) potential and emerging consumer issues which relate to digital platform services.

In the view of ADMA, mitigation of consumer, competition and other societal challenges associated with these issues requires a substantial lift in data maturity, data governance and associated assurance controls of many businesses, to bring their practices and processes up to emerging good practice. The lift in capabilities may be prompted by new legal requirements, and incentivised by legal exposures and potential penalties. However, having regard to the increasingly complex web of legal requirements as interpreted and applied by multiple regulators and bodies developing mandatory industry codes, a robust and effective compliance environment requires regulators to assist businesses to understand how to effect good practice process and practices across the increasingly complex web of regulatory requirements. That need is especially acute for small to medium businesses that engage in and depend upon data-driven marketing, but do not have either in-house capabilities or financial resources to navigate this increasingly complex web of legal requirements. This complexity is best addressed by using a coordination approach across each of the DP-Reg regulators. That is, coordination between the ACCC, ACMA, eSafety Commissier, and the OAIC, and in particular through issue of joint guidance materials that assist businesses to navigate these requirements. Close coordination will also assist effective enforcement by the regulators and regulatory predictability for the regulated.

The DP-Reg (ACCC, ACMA, eSafety Commission, and OAIC) has already demonstrated that it can issue joint communiques.[1] It would be reasonable to expect that enforcement coordination between the regulators could extend to guidance. Drafting guidance can be supported by industry and industry associations. In turn, this can lead to industry association reinforcement of that guidance.

It is useful to provide a case study as to how this might work. The ACMA has consulted on its views on the use of consumer consent to provide guidance to businesses that undertake email, SMS, and telephone marketing. Having drafted expectations that took into account industry best practice, the ACMA published these.[2] ADMA has promoted that statement of expectations.[3]

3 Dark patterns

The emergence and proliferation of 'dark patterns' in digital platforms and services represent a growing concern for consumers, regulators, and responsible businesses alike.

Reflecting the approach taken in the ACCC's Digital platform services inquiry Interim report No. 2 on app marketplaces, the OECD[4] defines Dark Patterns as techniques used in the design of websites and apps to take advantage of behavioural biases to coerce, steer, or deceive consumers into making unintended and potentially harmful decisions.

More recently, the European Data Protection Board has published guidelines on dark patterns in social media platform interfaces.[5] This sets out six classes of dark pattern with 17 specific patterns.

3.1 Examples of Dark Patterns in Advertising

Dark patterns manifest in various forms within the advertising landscape, including but not limited to:

- **Stirring** affects the choice users would make by appealing to their emotions or using visual nudges**.** It includes:
    - **Confirmshaming** (or emotional steering) which employs guilt-inducing or manipulative language to pressure users into opting into data collection or sharing practices; and
    - **Hidden in plain sight** which is the use of a visual style which could nudge user toward less restrictive information or data protection controls;
- **Hidden Costs** which conceal or downplays additional charges or fees associated with a product or service until late in the user journey;
- **Trick Questions** such as phrasing questions or consent requests in a misleading or confusing manner to elicit unintended or unwanted user responses;

[1] https://www.accc.gov.au/about-us/news/media-updates/communique-digital-platform-regulators-forum-2024 accessed 17 August 2024.
[2] https://www.acma.gov.au/articles/2024-06/consent-expectations-businesses-using-direct-marketing accessed 17 August 2024.
[3] https://www.adma.com.au/key-compliance-acma-fy25-what-you-need-know accessed 17 August 2024.
[4] OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en.
[5] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en accessed 22 August 2024.

- **Forced Continuity** which is making it difficult or overly complicated for users to cancel subscriptions or opt-out of services, often requiring multiple steps or hidden options;[6]
- **Bait and Switch** in which a product or service is advertised at an attractive price or with certain features, only to reveal terms or conditions which are less appealing later in the process; and
- **Privacy Zuckering** which employs deceptive design practices to nudge users into sharing more personal information than they intend or are comfortable with.

Similar deceptive practices can be labelled differently. The common characteristic is that the effect is to deceive consumers. The phenomenon of dark patterns is economy-wide and not confined to online (virtual) environments: many bricks and mortar floor store layouts also effect data patterns. That noted, availability of range and depth of data about individual consumers (whether or not identifiable) garnered through online activity and transactions of those individual consumers enhances an advertiser's ability to create personalised ads that use features to *specifically appeal* emotionally or psychologically to its intended target.

Dark patterns appear in two digital environments.

The primary one is the design of customer interactions to deceive customers to follow a specific path.

The second and distinct one relates to obtaining consent. This is the use of dark patterns to obtain consent from a customer who would not reasonably provide it.

Both of these practices are problematic.

These two applications of dark patterns indicate an issue which is found in many aspects of the digital economy. There may be a need for legislative changes in multiple pieces of legislation enforced by ACCC, ACMA, eSafety Commissioner, and OAIC to address a specific issue. Where, the use of dark patterns to obtain consent may not be in the course of trade or commerce, the effect is that a prohibition may need to be in place in the Privacy Act and Online Safety Act, as well as in the Australian Consumer Law.

3.2 Impact on Consumers and the Industry

Dark patterns not only undermine consumer trust and confidence in digital platforms and services, but also distort the competitive landscape by rewarding those who engage in manipulative practices. They erode the foundations of a healthy, competitive, and sustainable digital advertising ecosystem. Elimination of dark patterns is a necessary precondition for transparency, fairness, and respect for user autonomy.

3.3 International Regulatory and Policy Responses

Recognising the detrimental effects of dark patterns, several international regulators and policymakers have taken steps to address this issue:

3.3.1 European Union

The General Data Protection Regulation (**GDPR**) includes provisions aimed at enhancing transparency and user control over personal data processing, which can indirectly mitigate the impact of certain dark patterns. The Digital Services Act (**DSA**), recently adopted by the EU, explicitly prohibits dark patterns that impair user autonomy or distort their decision-making processes.

[6] This issue and the problems flowing from it are well described in the Consumer Policy Research Centre's August 20, 2024 report "Let Me Out – Subscription trap practices in Australia". Available at https://cprc.org.au/report/let-me-out accessed 22 August 2024.

3.3.2 United States

The Federal Trade Commission (**FTC**) has actively pursued enforcement actions against companies employing dark patterns, emphasising the importance of clear and conspicuous disclosures, meaningful choices, and easy opt-out mechanisms.

California's Consumer Privacy Act (**CCPA**) also includes provisions against dark patterns that interfere with consumer privacy choices.

3.3.3 Australia

While there is no specific legislation addressing dark patterns, the ACCC has taken action against companies engaging in misleading or deceptive conduct online, which can encompass certain dark pattern practices.

The recommendation by the ACCC to address unfair trading practices, will also provide the basis for regulatory enforcement against dark patterns.

The Australian Privacy Principles (**APPs**) also provide a framework for ensuring fair and transparent handling of personal information. On 24 July, the OAIC announced the results of research on deceptive design to influence privacy choices.[7]

3.4 Recommendations

To combat the pervasive use of dark patterns in the digital advertising sector, ADMA suggests consideration of the following:

- Establish clear definitions and guidelines outlining specific dark pattern practices that are considered unacceptable or unlawful, providing clarity for businesses and consumers alike.
- Empower regulatory bodies to investigate and take action against companies that employ dark patterns, including imposing fines or other penalties.
- Provide, and work with other authoritative voices that provide, education to digital marketers on industry best practices to identify and stop the use of dark patterns, and to promote ethical online customer experience (CX) design.
- Educate consumers about dark patterns, their potential harms, and how to recognise and avoid them.
- Encourage collaboration between industry stakeholders, regulators, and consumer advocacy groups to develop innovative solutions and technologies to detect and mitigate the impact of dark patterns.

By adopting a multi-faceted approach that combines regulatory measures, industry self-regulation, consumer education, and technological innovation, we can create a digital advertising landscape that is free from deceptive design practices and empowers consumers to make informed choices.

4 Cookie deprecation

On 22 July 2024, Google announced that its plan to deprecate third-party cookies in 2025 had been postponed indefinitely.

This signals a significant shift in the digital advertising landscape as the industry has been anticipating this change for several years. The deprecation of third-party cookies is not new in the advertising landscape with

[7] https://www.oaic.gov.au/newsroom/gpen-sweep-finds-majority-of-websites-and-mobile-apps-use-deceptive-design-to-influence-privacy-choices accessed 17 August 2024.

Google being one of the last browsers to make this move. However, it symbolised the most significant shift in the landscape. Marketers began to prepare for a change in the way they managed audience segmentation, audience targeting and retargeting, lookalike modelling, measurement and attribution, distribution of marketing budgets, and multi-touch attribution. The preparation required for this future state, along with the need to better prepare for privacy reform, moved many marketers to focus on their first party data strategies. The announcement of the delay while providing some businesses more time to re-evaluate their approach to data collection and privacy is not likely to greatly impact the marketers that are preparing themselves for the requirements of privacy reform. Google's announcement indicated that it would be providing users with more control to opt out of third-party cookie tracking at the browser level. Provision of this option, if clear and transparent, will likely result in customers exercising this option anyway.

ADMA, representing best practice data-driven marketing and advertising in Australia, has consistently advocated for the collection and use of first-party data as a cornerstone of responsible and effective marketing practices. We believe that first-party data, collected directly from consumers, with their explicit consent, offers several advantages over third-party cookies.

4.1 Advantages of First-Party Data

1. First-party data collection, when coupled with transparent privacy practices and clear consent mechanisms, fosters consumer trust. Consumers are more likely to share their data when they understand how it will be used and have control over its collection.

2. First-party data, collected directly from consumers, is inherently more accurate and relevant than third-party data, which is often inferred or aggregated from various sources. This accuracy leads to more targeted and personalised marketing campaigns, improving the consumer experience and driving better results for businesses.

3. First-party data collection empowers a business to have greater control over the data the business holds and how this data is used. This control enables a business to tailor its marketing strategies to their specific needs and objectives, without relying on third-party intermediaries. Reliance upon first party data also substantially reduces the compliance risk for an entity that otherwise is inherent in collection and sharing of consumer data across multi-party digital marketing data ecosystems, because a business is able to focus upon accountability and compliance for its own practices, rather than endeavouring to assess, monitor, review or audit compliance of data practices of third parties.

4. As the digital advertising landscape continues to evolve, with increasing emphasis on privacy and consumer control, first-party data collection offers a sustainable and future-proof solution. Businesses that invest in building their first-party data capabilities will be better positioned to adapt to future changes in technology and regulation.

4.2 Sectoral Impact of Cookie Deprecation Delay

The delay in cookie deprecation presents both opportunities and challenges for the digital marketing sector.

On the one hand, it provides businesses with additional time to transition to first-party data collection and develop alternative targeting and measurement solutions.

On the other hand, for the less innovative and progressive marketers, it may create uncertainty and prolong the reliance on third-party cookies, hindering innovation and progress towards a more privacy-centric advertising ecosystem.

There is also an issue that flows from the proposed changes to privacy law. The over-arching 'fair and reasonable' test may mean that there is a regulatory view as to fairness or otherwise of particular uses of

third-party data. This regulatory view could be expressed via DP-Reg, rather than just the Privacy Commissioner. For example, this view may be that it is fair and reasonable for use of third-party cookies for highly differentiated marketing be consumer opt-in, rather than opt-out.

4.3 Recommendations

By embracing first-party data and prioritising consumer privacy, ADMA supports a sustainable, competitive, and thriving digital advertising ecosystem that benefits both businesses and consumers.

ADMA's industry best practice education urges businesses to seize this opportunity to prioritise the collection and use of first-party data. This includes guidance to:

- Embrace transparency and ensure that consumers understand how their data is collected, used, and shared. Provide clear and accessible privacy policies and obtain explicit consent for data collection.
- Develop robust first-party data collection strategies and invest in data management technologies to collect, store, and analyse data effectively.
- Investigate and adopt privacy-preserving targeting and measurement solutions, such as contextual advertising, cohort-based targeting, and differential privacy.
- Work with industry partners, including technology providers, publishers, and advertisers, to develop and implement privacy-centric solutions.

Regulatory frameworks should promote privacy, transparency, and consumer control while enabling responsible data-driven marketing and advertising.

We commend consideration by the ACCC of expression of support for this approach in the final report.

5 Definitions that flow from the definitions in the Privacy Act amendments

The Attorney General's Department (**AGD**) has conducted a Privacy Act Review. This review originated out of recommendations from the final report of ACCC's 2019 Digital Platforms Inquiry. The AGD released the Privacy Act Review Report in February 2023 and, subsequently undertook public consultation to inform the government response. On 28 September 2023, the Australian Government released its response to the Privacy Act Review Report. It is expected that the Government will introduce amendments to the Privacy Act during the 2024 Spring Sittings of Parliament.

ADMA supports most of the proposed changes to the Privacy Act as proposed in the AGD's Privacy Act Review Report of February 2023 and the Australian Government's response of 28 September 2023. ADMA considers that consumer trust in the digital marketing practices of a business drives overall consumer trust in the brand and in the digital economy, and regulation should be designed to facilitate trustworthy and responsible digital marketing practices and impede unfair or unreasonable uses and applications of consumer data.

5.1 Fair and reasonable

The Government has signalled a shift from the current framework of consent to an overarching determination of whether it is 'fair and reasonable' to collect, use and disclose the personal information in the circumstances. The test is a uniquely Australian approach that changes the current power imbalance to favour individuals. This test applies whether or not an individual has consented to the collection, use, and disclosure of their personal information.

In August to November 2023, Treasury consulted on a Regulation Impact Statement examining approaches to regulating unfair trading practices.[8] The submissions to that consultation have recently been published. However, the introduction of changes was an agenda item at the meeting of Commonwealth, State and Territory Consumer Affairs Ministers on Friday 24 November 2023. Ministers agreed on further work on 'protecting consumers and small business from unfair trading practices across the economy.'

It is likely that the definition of unfair trading practices will be legislated by amending the *Competition and Consumer Act 2010* (Cth) (**CCA**). Further, the CCA amendments are likely to be generally concurrent with the amendments to the Privacy Act.

The effect of this is that there will be an issue facing practitioners. This is the potential for discrepancies between what is 'unfair' as an 'unfair trading practice' and what is 'fair' in a 'fair and reasonable' test.

It makes sense for all of the DP-Reg regulators to distinguish between 'unfair' and 'fair', even if this simply results in guidance that 'fair' does not mean 'not unfair.'

The need to have clear guidance for industry to understand the boundaries of 'fair and reasonable' as to the collection, use and disclosure of data will be critical for industry to be able to operationalise privacy reform to deliver expected outcomes. Without any such guidance, and with the potential introduction of a direct right of action into the Privacy Act, there is a risk that 'fair and reasonable' could otherwise be determined by the court through a plethora of class action lawsuits. This would delay application and potentially undermine confidence

It would be useful for consistency across the DP-Reg regulators to consider reasonableness. Otherwise, there will be an absence of clarity as to whether the intent of the privacy reform legislation is for 'reasonable' to be a limitation of an obligation (as in this case) or something else.

This is an area where a change in the privacy law will create a change in the expectations of reasonable consumers outside of a privacy environment. Tying back to dark patterns, if a dark pattern fails the 'fair and reasonable' test in the context of obtaining consent, then there will be a reasonable expectation that a similar pattern will be prohibited in the context of trade and commerce.

This is another indication of the way that DP-Reg can act to ensure that the expectations of the regulated and their customers can be harmonised in an environment of legislative change.

5.2 Automated decision making

Consistent with EU law, the privacy law reforms will mean that entities subject to the law must provide a statement of types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on individuals rights. Individuals will have a right to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made.

Automated decision making has implications that are much broader that the privacy implications. It seems reasonable that the obligation to provide meaningful information should apply as a general consumer protection, potentially in the context of unfair trading terms.

From a traditional marketing perspective, this requirement is a shift in mindset for marketers (and businesses in general) prompting them to think upfront about their data practices (as opposed to collecting data and then determining what they may hope to do with it) This shift is a move to better and more responsible practices around data, collection, use and disclosure and aligns with the approach ADMA guidance has always taken towards responsible marketing. This higher level of transparency will not only instil more

[8] https://treasury.gov.au/consultation/c2023–430458 accessed 17 August 2024.

confidence from customers, and it will also help ensure that the process of data minimisation becomes standard business practice.

5.3 Consent

The requirement for obtaining consent is proposed to be consistent with Consumer Data Right (CDR) consent. That is, consent must be voluntary, informed, current, specific, unambiguous, and easily withdrawn. It must also be given using an unambiguous indication through clear action.

The issue that arises here is that consumer expectations will, and should, be that consent across regulatory regimes will have the same characteristics. This has implications for the work of 'likely to mislead or deceive' in section 18 of the Australian Consumer Law. That is, a consumer, acting reasonably, will have an expectation that consent will have the same meaning as that under privacy law. Approaches to non-privacy consent that are inconsistent with CDR consent framework are likely to be either misleading or deceptive. This is a further issue in which changes in once piece of legislation in the DP-Reg space will have an impact on other DP-Reg regulators.

5.4 Privacy reform - Proposal 20 – Direct marketing, targeting and targeted advertising

There are three definitions (direct marketing, targeting and targeted advertising) referenced in the proposed privacy reforms that will have direct effects on all four DP-Reg regulators.

The first (direct marketing) is outlined as the collection, use or disclosure of Personal Information (PI) to communicate directly with an individual to promote advertising or marketing material, including by mail, voice calls (and video calls), and commercial electronic messages (email, MMS, SMS).

This definition will interact with the ACMA's enforcement of the Spam Act and the Do Not Call Register Act.

The definition will also interact with the ACCC's enforcement of the Australian Consumer Law as it relates to advertising.

As part of a cost benefit analysis conducted by the Attorney Generals Department, there were some definitions presented that have the potential to form part of privacy legislation. One of these defined targeting and targeted advertising in a linked way. Targeting is outlined as evaluating PI for tailoring services, content, information, advertisements or offers provided to or withheld from an individual, either on their own, or as a member of some group or class, online. The word 'online' is an important element of this definition. In turn, Targeted Advertising is outlined as information designed to promote the message of an entity or individual, presented to an individual where targeting has been used. Individuals can opt-out of receiving Targeted Advertising but that opt-out is not required to be unqualified.

The effect is that the privacy reforms will create a clearer exchange of value for services which are supplied at no charge. In effect, individuals who opt out of receiving Targeted Advertising may receive a different (or no) service compare with those who do not opt out. This is a change from the earlier position in which opting out of Targeting (rather than receiving Targeted Advertising) was considered.

5.5 Opt-out of online targeted advertising

In relation to third-party targeted advertising, there may be a need to provide users with a general opt out mechanism.

5.5.1 Three levels of general opt out

Broadly, there are three levels at which a general opt out could be offered:

(a) at the browser level, where a signal could be initiated. This is standardised as Global Privacy Control (**GPC**);
(b) by facilitating the entry of a form of privacy intermediary (or intermediaries) known as a Consent Management Provider (**CMP**); or
(c) by creating a government-managed centralised system, similar to the Do Not Call Register, which could be thought of as a Do Not Track Register or Do Not Target Register.

In practice, a combination of these approaches might offer the best solution. For example, GPC could be used as a default signal, with CMPs providing more granular control for users who want it, and a government-backed system ensuring enforcement and accountability.

ADMA members are in a position to work with the chosen solution. However, the appropriate answer is not obvious. For example, GPC gives consumers the greatest choice, but imposes the burden of the associated technology. CMPs reduce the need for Commonwealth funding, but data intermediaries are (generally) opposed by consumer advocates (for example both Choice and the CPRC take this view). The ACCC has already gathered evidence on the risk posed data intermediaries and that may be sufficient to determine that CMP based solutions are not appropriate in Australia.

Set out in Table 1 is a selection of the pros and cons of each of the three approaches.

Table 1: Pros and cons of opt out approaches

Approach	Pros	Cons
Local (Global Privacy Control)	▪ Empowers users with a clear signal to opt out of the sale or sharing of their personal data for advertising purposes. ▪ Can be applied across websites and platforms, potentially offering broader protection than individual consent mechanisms. ▪ Provides a consistent signal for businesses to comply with, simplifying the opt-out process.	▪ Requires widespread adoption by websites, browsers, and advertisers to be truly effective. ▪ May face challenges with enforcement and ensuring businesses respect the signal. ▪ Implementation may require technical expertise for both users and websites.
Intermediated – Consent Management Providers	▪ Allows users to customise their consent choices for different types of data and purposes. ▪ Can provide clear information about how data is used and shared. ▪ Can be adapted to different legal and regulatory frameworks.	▪ Can be overwhelming for users due to the sheer number of choices and complexity of settings. ▪ Some CMPs may be influenced by commercial interests, potentially favouring certain advertisers or data practices. ▪ Lack of standardisation can lead to different experiences across websites and platforms.
Government-Managed Centralised System (Do Not Track/Target Register)	▪ Government backing can ensure better compliance and enforcement of user preferences. ▪ Easier for users to understand and use, as it involves a single opt-out mechanism. ▪ Provides equal protection for all users, regardless of their	▪ Raises potential privacy risks due to the centralised collection of user data. ▪ Requires significant government resources to develop, maintain, and enforce. ▪ May face resistance from international players due to a requirement for localisation

Approach	Pros	Cons
	technical knowledge or ability to navigate complex settings.	that is unique to Australia.

ADMA takes the view that if the proposal relating to opting out of third-party advertising is to go ahead that the OAIC must provide guidance on the best mechanism to provide a general opt out to third-party targeted advertising. It is likely that this guidance will be most effective if it both has input from industry (so as to obtain use case examples) and is coordinated with other DP-Reg regulators. ADMA takes this position on the basis that each of the DP-Reg regulators will need to enforce in the context of the preferred solution.

5.5.2 Opt in/out by delivery mechanism

In respect of in-channel advertising, there will still be a need for options for consumers. This includes the ability (option) for a consumer to opt out of all commercial communications from a brand. However, it is likely that some consumers will be comfortable with (have a preference for) some delivery mechanisms and not others. For example, a consumer might be comfortable with a commercial message being delivered on one platform (for example, internet browser), but not comfortable with an email, or an SMS. ADMA favours consumer choice. That is, the ability for consumers to elect to opt in, or out, of commercial messaging by specific delivery mechanisms, or as a whole.

5.6 Trading

The eighth interim report for the Digital Platform Services Inquiry, released by the ACCC on 21 May 2024 addressed the role that data firms play in the economy. The issues raised, particularly in respect of the scope of data firms, are reflected in the proposed changes to privacy law.

As ADMA understands things, the privacy law changes will introduce the concept of controllers and processors of information. These concepts are widely adopted elsewhere in the world. Controllers are entities that determine the purposes and means of how personal information is collected, used and disclosed. Processors are entities that collect, use or disclose personal information on behalf of the documented instructions of a Controller.

In that context, the proposed definition of 'Trading' is the commercial disclosure of information that enables an entity to target, contact or geolocate a unique transactor, including where that transactor is not otherwise reasonably identifiable, but not transfers of PI between a Controller and a Processor (on the basis that this is a 'use' of PI, not a 'disclosure').

In ADMA's view, this is consistent with the ACCC's approach of a very broad definition of data firm. One issue that each of the DP-Reg regulators will face in their specific enforcement actions is regulated entities claiming to be Processors in order to avoid the stricter consumer expectations of the obligations on Controllers.

5.7 Personal Information

As ADMA understands the Government's position, the definition of Personal Information (**PI**) will be broadened to include information which *relates to* a reasonably identifiable individual instead of simply information 'about' an individual. In this context, PI may include information such as location data, inferred information, and technical or behavioural data (note this is a non-exhaustive list). We also understand that factors to take into account when determining whether the risk of identifiability is higher than *low or remote* will include factors such as: the nature and volume of the information, who holds or has access to the information, how and why the information is collected, used, stored and disclosed, any other information that is available (or may reasonably become available) to the recipient, and the practicability of using that information to identify an individual, and the context in which the information is handled and/or disclosed.

The issue for the ACCC and other DP-Reg regulators to consider is that this means that some of the currently used privacy enhancing technologies, discussed in the next section, may not de-identify to the extent required by the new definitions. ADMA is providing services to its members to understand these issues and to ensure that their use of privacy enhancing technologies is at best practice and complies with the proposed definitions. However, the changes mean that claims made by businesses regarding privacy in the past, may not be correct in the future.

6 Adoption of privacy enhancing technologies (PETs)

Privacy Enhancing Technologies (**PET**s) are a suite of tools and techniques designed to enable data processing and analysis while minimising the risks to individual privacy. PETs encompass a broad spectrum of solutions, including anonymisation, pseudonymisation, differential privacy, homomorphic encryption, secure multi-party computation, and federated learning.

6.1 Current Adoption of PETs in Australia

The adoption of PETs in Australia has been steadily increasing, driven by a growing awareness of privacy and consumer protection concerns among consumers and businesses, as well as evolving regulatory requirements. Digital platforms, such as Google, have played a crucial role in promoting the use of PETs by offering built-in privacy features and tools.

However, the adoption of PETs is not uniform across industries and sectors. While some organisations have actively embraced PETs to enhance their privacy practices, others remain hesitant due to perceived technical complexities, cost implications, or lack of awareness.

6.2 Potential Impact of Regulatory Changes

Upcoming changes in privacy law in Australia, particularly those related to data minimisation, purpose limitation, and individual control over personal information, could significantly impact the effectiveness of certain PETs. For instance, if the law requires explicit consent for specific data processing purposes, techniques like anonymisation or pseudonymisation may not be sufficient to ensure compliance if the data can be re-identified or linked back to individuals.

Similarly, if the law imposes stricter requirements for data retention and deletion, certain PETs that rely on storing or processing personal data for extended periods may need to be re-evaluated or adapted.

We have already seen signalling on this from the US FTC. On 29 July 2024, the FTC issued a Technology Blog.[9] In summary the blog finds:

> *One way that companies obscure personal data is through 'hashing.' A hash by itself cannot easily be used to guess what the original data was. For this reason, companies often use hashing in cases where they are uncomfortable writing down or sharing the directly identifying data, but they still want to be able to store the data for matching against later. Companies often claim that hashing allows them to preserve user privacy. This logic is as old as it is flawed – hashes aren't 'anonymous' and can still be used to identify users, and their misuse can lead to harm. Companies should not act or claim as if hashing personal information renders it anonymised. FTC staff will remain vigilant to ensure companies are following the law and take action when the privacy claims they make are deceptive.*

[9] https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous access 17 August 2024.

6.3 Recommendations

To ensure the continued adoption and effectiveness of PETs in the evolving privacy landscape, we recommend the following:

- Provide clear guidance on the use of PETs in compliance with privacy laws, including specific requirements for different types of PETs and data processing activities.
- Encourage collaboration between industry stakeholders, technology providers, and regulators to develop and promote best practices and standards for the implementation and use of PETs.
- Invest in research and development to advance the capabilities of PETs, particularly in addressing challenges related to data minimisation, purpose limitation, and individual control.
- Raise awareness among businesses and consumers about the benefits and limitations of PETs, empowering them to make informed choices about privacy. This is a role that ADMA embraces.
- Design regulations with flexibility to accommodate the evolving nature of PETs in order to encourage innovation in privacy-preserving technologies.

6.4 The path forward

PETs offer a promising pathway to reconcile the benefits of data-driven innovation with the imperative of protecting individual privacy. By fostering a supportive regulatory environment, promoting industry collaboration, and investing in research and development, we can ensure that PETs continue to play a vital role in shaping a privacy-centric digital future for Australia.

It is important to recognise that PETs are not a silver bullet solution to all privacy challenges. They should be used in conjunction with other privacy-enhancing measures, such as transparent data practices, robust consent mechanisms, and strong data security protocols. By adopting a holistic approach to privacy, we can build a digital ecosystem that fosters trust, empowers individuals, and unlocks the full potential of data-driven innovation.

There are specific federation issues in the US which led to the FTC issuing guidance, rather than a privacy regulator. However, this reinforces the issues that flow from a multi-regulator environment. ADMA takes the view that this is another area where consultations and guidance at the DP-Reg level, as well as the level of each regulator, will reduce both regulatory over-reach and regulatory under-reach. In order to assist the creation of such guidelines, ADMA has worked with members to ensure that marketers understand PETs. This includes a webinar and other guidance. ADMA takes the view that informed marketers will be best positioned to engage in relevant regulatory conversations.

7 Growth in artificial intelligence

Artificial Intelligence (**AI**) has rapidly emerged as a transformative force in the marketing and advertising sector, changing how businesses engage with consumers, personalise experiences, and optimise campaigns. AI-powered tools and technologies are being used in various aspects of marketing and advertising, including:

- AI enables the collection, processing, and analysis of vast amounts of data, providing valuable insights into consumer behaviour, preferences, and trends.
- AI algorithms can segment audiences based on various criteria, enabling more targeted and personalised advertising campaigns.

- AI can generate and optimise content, including ad copy, social media posts, and product descriptions, to improve engagement and conversion rates.
- AI-powered programmatic advertising platforms automate the buying and selling of ad space, enabling real-time bidding and optimisation.
- AI-powered chatbots and virtual assistants provide personalised customer service and support, enhancing the customer experience.

7.1 Hyper-Personalised Advertising: Opportunities and Concerns

One of the most significant applications of AI in marketing and advertising is hyper-personalised advertising, which involves tailoring ads to individual users based on their unique characteristics, interests, and behaviours. Hyper-personalised advertising offers numerous benefits, including:

- By delivering ads that are highly relevant to individual users, hyper-personalised advertising can significantly improve engagement and conversion rates.
- Hyper-personalised advertising can create a more seamless and personalised customer experience, fostering loyalty and trust.
- By targeting ads more precisely, hyper-personalised advertising can improve the efficiency and return on investment (**ROI**) of marketing campaigns.

However, hyper-personalised advertising also raises significant privacy concerns, including:

- Hyper-personalised advertising often relies on collecting and processing large amounts of personal data, including browsing history, online purchases, social media activity, and location data, to create detailed user profiles.
- Consumers may not be fully aware of the extent of data collection and profiling or have meaningful control over how their data is used for advertising purposes.
- AI algorithms used for hyper-personalised advertising may inadvertently perpetuate or amplify existing biases and discrimination in society.

7.2 Recommendations for Responsible AI Implementation

To ensure that the growth of AI in the marketing and advertising sector benefits both businesses and consumers, ADMA recommends the following:

- Provide consumers with clear and accessible information about how their data is collected, used, and shared for advertising purposes. Empower consumers with meaningful choices and control over their data and advertising preferences. This is consistent with proposed privacy reforms.
- Collect and process only the minimum necessary personal data for specific and legitimate advertising purposes. Avoid excessive data collection and profiling that may infringe on consumer privacy.
- Ensure that AI algorithms used for advertising are fair, unbiased, and do not discriminate against individuals or groups based on protected characteristics.
- Implement mechanisms to ensure accountability and explainability in AI-powered advertising systems, enabling consumers to understand and challenge automated decisions that affect them. As set out above, this is consistent with the proposed privacy approach to automated decision making.

- Foster collaboration between industry associations, regulators, and consumer advocacy groups to develop and promote best practices for the responsible use of AI in marketing and advertising.

By embracing these principles, the sector can harness the potential of AI to create a more effective, personalised, and privacy-respecting advertising ecosystem that benefits both businesses and consumers.

AI regulation cannot be stand-alone. It needs to have the context provided by the laws that the DP-Reg regulators enforce. The effect is that each regulator will need to deal with AI in the context of the way that it is used by regulated businesses in their sector. For example, deepfakes have been problematic in cyber-bullying as identified by the eSafety Commissioner.[10] In the position taken by the eSafety Commissioner, there are examples of the use of deepfakes in fraud. This could be in spam and scam SMS (dealt with by the ACMA) or misrepresentation (enforced by the ACCC). It could also be used as part of identity fraud (partially enforced by the OAIC). A single piece of AI legislation is unlikely to be able to address each and all of these issues. AI regulation needs to be in the hands of the regulators with relevant enforcement experience associated with their regulation. That is, the best outcome will be if AI legislation is in a Bill of consequential amendments.

This is an area where all four of the DP-Reg regulators have an interest. It is also one where a harmonised regulatory approach can promote the adoption of best practices.

8 International decisions on biometrics

The increasing use of biometrics across various sectors, including marketing and advertising, has prompted a wave of regulatory changes globally, aimed at safeguarding individual privacy and ensuring responsible use of this sensitive data. While Australia has not seen any significant regulatory changes in this domain, the international landscape provides valuable insights and potential lessons for future policy development.

8.1 Key Regulatory Trends in Biometrics

- A common thread across many jurisdictions is the emphasis on explicit consent and purpose limitation for the collection and use of biometric data. Individuals should be clearly informed about the purpose of data collection, how it will be used, and with whom it may be shared.
- Regulatory frameworks increasingly mandate the collection and retention of only the minimum necessary biometric data for the specified purpose and for the shortest possible duration.
- Stricter requirements for the secure storage and transmission of biometric data are being implemented, along with obligations for organisations to be transparent about their data practices and provide individuals with access to their biometric data.
- Some jurisdictions have introduced specific regulations governing the use of biometrics in certain contexts, such as facial recognition technology in public spaces or for law enforcement purposes. Prohibitions on certain uses of biometrics, such as discriminatory profiling or surveillance, are also becoming more common.
- The establishment of dedicated regulatory bodies or the expansion of existing agencies' powers to oversee and enforce biometric data protection regulations is gaining traction in several jurisdictions.

[10] https://www.esafety.gov.au/industry/tech-trends-and-challenges/deepfakes accessed 23 August 2024.

8.2 Examples of International Regulatory Frameworks

8.2.1 European Union

The General Data Protection Regulation (**GDPR**) categorises biometric data as a special category of personal data requiring heightened protection. It mandates explicit consent, purpose limitation, data minimisation, and robust security measures.

8.2.2 United States

While there is no comprehensive federal law governing biometrics, several states have enacted biometric privacy laws, such as the Illinois Biometric Information Privacy Act (**BIPA**), which imposes strict requirements on the collection, use, and storage of biometric data.

8.2.3 Canada

The Personal Information Protection and Electronic Documents Act (**PIPEDA**) considers biometric data as sensitive personal information and requires organisations to obtain meaningful consent, limit collection and use to specific purposes, and implement appropriate safeguards.

8.2.4 Other OECD Countries

Many OECD countries have incorporated biometric data protection provisions into their broader privacy laws, often mirroring the principles of the GDPR.

8.2.5 United Kingdom

The UK's Data Protection Act 2018, which implements the GDPR, also provides specific guidance on the use of biometrics, particularly in the context of law enforcement.

8.3 Implications for Australia

The international regulatory landscape on biometrics underscores the growing importance of protecting this sensitive data. As Australia navigates the increasing use of biometrics in various sectors, including marketing and advertising, it is imperative to consider aligning our regulatory framework with international best practices.

We recommend the following:

- Amend the *Privacy Act 1988* (Cth), to address the specific challenges posed by biometric data. That is, as part of the currently proposed reforms, incorporate explicit provisions on consent, purpose limitation, data minimisation, security, and transparency.
- Develop sector-specific guidelines or codes of conduct for the responsible use of biometrics in marketing and advertising, taking into account the unique challenges and opportunities presented by this technology. These guidelines would, ideally, be at DP-Reg level. If not, it is essential that there is consistency between DP-Reg regulators. Once these guidelines are issued, the Office of the Australian Information Commissioner (**OAIC**), must enforce biometric privacy regulation.
- Raise public awareness about biometric data, its potential benefits and risks, and individuals' rights and choices regarding its collection and use. It is appropriate that businesses and government entities that collect biometric data should fund public awareness and education.

8.4 The path forward

The global trend towards stricter regulation of biometrics reflects a growing recognition of the need to balance the potential benefits of this technology with protection of individual privacy.

Collected biometric data is likely to be 'personal information' or 'sensitive information,' as defined under section 6 of the *Privacy Act 1988* (Cth). Sensitive information receives a higher degree of protection under the Privacy Act. The proposed changes to the Privacy Act are likely to mean that collection of biometric data represents a 'high risk privacy activity.'

However, it is also likely that collection of biometric data would also fall under other law and regulations enforced by regulators in DP-Reg. In particular, the use of facial recognition technologies may lead to issues under both Australian Consumer Law and the Online Safety Act.

This is a further area where inquiry, consultation, and guidance at the DP-Reg level may assist the regulated entities.

9 Role of ADMA

ADMA's primary role is to be an industry resource for responsible, effective and creative data-driven marketing across all channels and platforms. ADMA provides thought leadership in best practice, insights, ideas, and innovation for the marketing industry. This is in the context of data-driven marketing practices with the understanding that the marketing department drives growth of businesses. It provides education and guidance in responsible marketing practices to help marketers lift their data- driven processes and practices for the betterment of their customers, building consumer trust.

ADMA helps marketers keep up with what's going on with new and developing laws, inquiries, and reports into our industry. It does this by having both member-only and publicly available content to help marketers comply with Australian and international regulations.

Our work includes news stories, content, webinars, masterclasses and training courses (including in-house training for marketing teams) to keep the data-driven marketing community up to date with compliance issues. The ADMA regulatory working group communicates on behalf of data-driven marketers to governments and regulators. We cover topics such as privacy, data handling, running trade promotions, best practices for making claims when advertising or marketing, compliance in relation to electronic communications and telemarketing, and understanding changing technology practices such as third-party cookies.

We aim to keep our members, and the wider industry informed in the regulatory space and help marketers understand how to both prioritise best practice and apply it right through to the frontline of a business. This is part of facilitating understanding of best practice for members and beyond. ADMA continues to work with each of the DP-Reg regulators to ensure that compliance in an environment of change is part of that best practice.