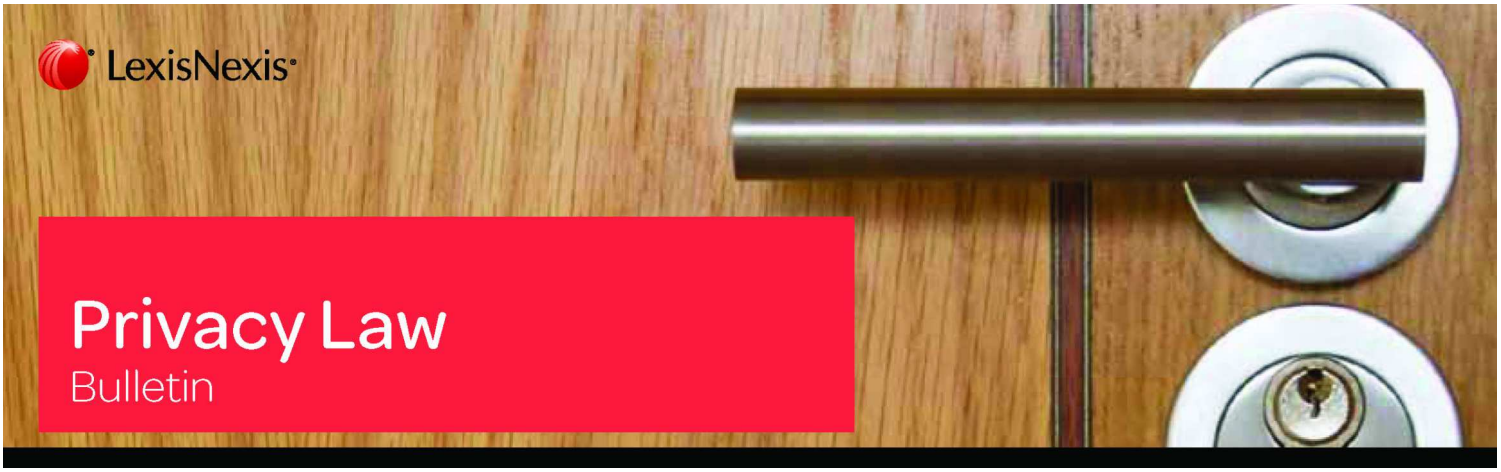

Privacy Law Bulletin

2024 . Vol 21 No 1

Contents

page 2 **The intersection between privacy, business and marketing law**
Sharon Givoni *SHARON GIVONI CONSULTING*

page 4 **Interview with Andrew Hii — Partner, Gilbert + Tobin**
Interview by ***Sharon Givoni*** *GENERAL EDITOR, PRIVACY LAW BULLETIN*

page 9 **Targeted advertising and profiling — charting a new course in Australian privacy law and regulation**
Peter Leonard *DATA SYNERGIES AND UNSW BUSINESS SCHOOL*

page 19 **"No junk mail" — a privacy-first/first-party data approach to digital marketing**
Alec Christie *CLYDE & CO*

page 23 **Click "Accept All" to these new privacy reforms**
Andrea Beatty, ***Jennifer Fu*** *and* ***Jack Shaw*** *PIPER ALDERMAN*

Information contained in this newsletter is current as at April 2024

The intersection between privacy, business and marketing law

Sharon Givoni *SHARON GIVONI CONSULTING*

When Google was launched in 1998, it was predicted to quickly fail.

Conventional business wisdom at the time was that Google's business model was flawed because it gave its users access to its services for free. The scepticism stemmed from the prevailing belief that internet companies, especially search engines, should charge users for access or rely on the placement of large, indiscriminate, untargeted advertising banners on pages.

However, Google succeeded and became one of the fastest-growing companies in corporate history. Today, only 25 years later, it has an annual turnover of $309.39 billion. It did this by developing a new advertising model that only displayed relevant advertising alongside search results.

The Google model, now commonplace in online commerce, was the harvesting and use of personal information of users to facilitate highly targeted marketing to that user based on their likes or wants, with a high guarantee of user interest, for which companies wishing to market their products or services would pay a premium.

Far from not having a monetisation strategy requiring payment for use, Google knew the power of the personal information they collected from their users and how this could be turned into the new "rivers of gold" in advertising revenue.

Highly visible, for perhaps the first time, was the inherent friction between the individual's privacy in the form of their personal information and the thirst of marketers to get their message front and centre in the face of the individuals.

In this rapidly evolving digital commercial landscape, the juncture between privacy law and marketing practices stands as is now a pivotal area of focus for lawyers.

In the realm of Australian privacy law, especially when advising clients in the area of marketing and privacy law compliance — from spam to opt-outs and comprehensive retail strategies — an integrated understanding is useful.

This encompasses not just the legal framework and marketing principles, but also the intricacies of the technologies propelling online marketing, which is becoming increasingly pervasive in our everyday lives.

One key area, behavioural advertising, as exemplified by Google, showcases this interplay, as it hinges on collecting, compiling and analysing user behaviour to formulate targeted and often intrusive advertising campaigns.

Here, the pressing issue for lawyers may be negotiating the limits of user profiling within the confines of the Australian Privacy Act 1988. In the realm of data analytics and big data, as lawyers, we also find ourselves at the forefront of guiding businesses through the complexities of big data utilization for market research and consumer insights. This calls for a keen understanding of the legalities surrounding the gathering, storage, and examination of expansive personal data sets.

Here, the pressing issue for lawyers may be negotiating the limits of user profiling within the confines of the Privacy Act. Can clients legally collect personal information without explicit consent? Can they track users' online activities across different websites to build comprehensive profiles?

Lawyers must also consider whether their clients can use predictive analytics to infer sensitive information about individuals, such as health conditions or political affiliations, based on seemingly innocuous data. And can businesses share these profiles with third parties for broader marketing purposes or integrate this data with information from public sources?

Then there is data analytics and big data.

As lawyers we also find ourselves at the forefront of guiding businesses through the complexities of big data utilisation for market research and consumer insights. This calls for a keen understanding of the legalities surrounding the gathering, storage and examining expansive personal data sets.

Furthermore, the explosive growth of social media marketing necessitates a comprehension of the privacy implications inherent in the use of using vast quantities

of personal data. So many businesses are leveraging tools and technologies that track user activities across platforms — analysing likes, shares, comments and posts to glean insights into preferences and interests, as well as employing cookies and pixel tags to monitor browsing habits and online interactions. Peoples' user-generated content also provides a rich source of personal details and lest we forget location data, showing patterns in movements and lifestyle choices. Collectively, these methods paint a comprehensive picture for targeted marketing.

Legal professionals are tasked with ensuring proper consent mechanisms are in place for marketing purposes and setting out the protocols for sharing such information with third parties, within the limits set by the Privacy Act.

This edition sets out to unravel the complex tapestry of marketing innovations intertwined with privacy laws, both legislatively and at common law, charting the historical path of online marketing to shed light on our present state and future challenges.

The emergence of terms like tracking technology, hyper-targeted advertisements and predictive analytics into common parlance signifies highlights the advanced tactics employed in modern marketing campaigns.

The core issue, however, reaches beyond simple consent — it probes into consumers' awareness regarding the use and monetisation of their personal data.

Yet, in my view, the crux of the challenge extends beyond the mere issue of consent.

Consumers' often have limited comprehension of how their data is harvested, used and capitalised upon. This is something that needs to be explored in more detail and begs the question — the integration of technology into our daily lives but generally have limited comprehension of how their data is harvested, used and capitalised. Given the integration of technology into our daily lives, this needs to be explored in more detail, and it begs the question — what is the line between convenience and intrusion?

For legal practitioners, this landscape necessitates a proactive stance towards privacy protection, ensuring that consumers' rights are safeguarded in the face of despite relentless technological advancements.

Simultaneously, from a legal advisory perspective, there is a need for lawyers to equip data-driven businesses — including online retailers — with the knowledge to navigate the legal intricacies of marketing practices to help them prevent potential privacy infringements.

As we explore this theme in this issue of the *Privacy Law Bulletin*, our aim is not only to provide legal professionals with insights into the historical context and current state of play but also to offer guidance on maintaining the delicate balance between new marketing practices and the protection of individual privacy and human autonomy.

Marketing and privacy law are now increasingly intertwined.

With the massive technological advancements in AI and quantum computing that can analyse vast amounts of data so much faster than traditional computers, the friction between the two will inevitably become more and more pronounced. Consumers have learnt that the price of convenience is often the forfeiture of privacy and the question being asked is — how much are we willing to pay?

All of this can lead to a legal and customer-based landscape fraught with danger for the marketer, both in terms of customer satisfaction and legal compliance.

Welcome to an exploration of the dynamic interface between marketing, technology and law, where the quest to understand and navigate this terrain becomes more pertinent than ever.

General Editor's note

The Editor wishes to acknowledge Michael Rivette for his input and contribution towards the writing of this piece.

Sharon Givoni
Principal
Sharon Givoni Consulting
sharon@iplegal.com.au
www.sharongivoni.com.au

Interview with Andrew Hii — Partner, Gilbert + Tobin

Interview by ***Sharon Givoni*** *GENERAL EDITOR, PRIVACY LAW BULLETIN*

As Australia stands on the cusp of what is probably the most significant overhaul of its privacy laws since 2014, the intersection of marketing and privacy law emerges as a critical area of focus. In anticipation of these sweeping changes, we engaged with Andrew Hii, a privacy and data specialist at Gilbert + Tobin, to explore the specific impacts of the upcoming reforms on marketing practices.

The forthcoming reforms, as outlined in the *Privacy Act Review*[1] Report and set for a phased implementation starting from 2024, signal what might be a substantial change in how personal information is handled, especially in the context of marketing. These changes, while bringing Australian law into closer alignment with international standards like the General Data Protection Regulations (GDPR) and California Consumer Privacy Act 2018 (CCPA), also pose unique challenges and opportunities for Australian businesses engaged in marketing activities.

In this interview, Andrew Hii offers his expert insights into how these privacy law reforms may reshape marketing strategies. He delves into the nuances of the "unqualified right to object" in direct marketing, the redefined parameters of "valid consent" and the broader implications of an expanded definition of personal information.

Andrew addresses the operational challenges businesses may face, the strategic adjustments required in direct marketing campaigns and the critical role of consent in customer engagement. Furthermore, he explores the intersection of privacy laws with social media marketing strategies, offering guidance on how businesses can adapt to these changes while maintaining compliance and consumer trust.

This interview with Andrew Hii is focused on exploring the intricate interplay between marketing and privacy law with insights for legal practitioners to help their clients navigate the complexities of marketing in a privacy-conscious world.

Q: Given that Australia's proposed "unqualified right to object" aligns more closely with international regulations like GDPR and CCPA, how do you think this will impact Australian businesses, especially in terms of international collaborations or partnerships?

I would characterise Australia's proposed "unqualified right to object" reforms as being relatively modest. They would extend the current [Australian Privacy Principles] (APP) 7 rules that allow a person to request not to receive direct marketing communications. In a practical sense, I would expect that Australian business ought to be able to adapt to these new rules. If a business is unable to do so, then that is probably revealing a deeper problem with the way that the business handles personal information and marketing consents. The biggest system change I would expect to be required to be implemented is that systems will need to be put in place that ensure "opt-out" notices from customers are actioned, and how this "opt-out" will be treated alongside other interactions between the business and the individual. I'd expect that businesses would have little commercial interest in sending direct marketing to individuals who have clearly expressed a desire not to receive marketing information — so in that sense, I would expect the interests of both business and individuals to be aligned.

Q: In the context of the Privacy Act Review Discussion Paper, there are concerns raised about the validity of consent. Can you elaborate on what constitutes "valid consent" in direct marketing, and how might this change with the proposed amendments?

It is relatively uncontroversial that, in theory, consent should be voluntary, informed, specific, current and given by a person with capacity. This is codified in the GDPR, but not similarly codified in the Privacy Act 1988 (Cth).

While this might be easy to express in principled terms, in practice, it can often be difficult to apply this in action. Consent in the context of direct marketing is a good example of this.

The concern in direct marketing is that:

- consent to receive direct marketing is bundled with other consent (eg, in agreeing to the terms and conditions to receive the relevant goods and services, the consumer is also consenting to receive direct marketing at the same time)
- when given in this bundled manner, consumers are not aware they are consenting to receive direct marketing
- consumers are not aware of what kinds of direct marketing they are consenting to receive
- consent is not periodically renewed

Lastly, capacity issues arise where direct marketing is conducted in respect to children.

The proposed amendments will likely change the way the consent for direct marketing may be sought and obtained. This includes when consent is initially obtained and a requirement to refresh consent periodically. Much stricter rules will apply in respect of direct marketing to children — including that any such direct marketing must be in the child's "best interests". While this "best interests" test is well-known in other areas of law, when applied in this context, it may be difficult to pass in many contexts.

To date, many companies rely upon the customer's initial acceptance of terms and conditions (for example, by checkbox on an online process) to authorise the future direct marketing that the company may wish to conduct. However, it is likely that direct marketing consent will need to be separated from acceptance of principal terms and conditions (which many companies already do), and that this consent will need to be more explicit in describing what forms of direct marketing will be conducted (which many companies do not do). Further, companies will need to establish processes by which they can periodically refresh consent — this is something that is relatively uncommon in Australia.

However, I do wish to make clear that the Government is not proposing that consent be obtained before any direct marketing be conducted, where the personal information was collected by the company from the individual. Consistent with what the Privacy Act currently provides, companies can collect personal information for direct marketing without express consent. However, they will be required to provide an unqualified opt out (and cannot use sensitive information).

The government has recognised that these general principles may be difficult to apply in practice, and that this is an area where it would be appropriate for the regulator to provide guidance. Under Proposal 11.2, the [Office of the Australian Information Commissioner] (OAIC) will be given the power to develop guidance on how online services should design consent requests. How useful this will be to businesses wishing to conduct direct marketing remains to be seen.

Q: The proposals aim to expand the definition of personal information to include technical identifiers and data, bringing targeted advertising under its purview. In your view Andrew, how might this broader definition affect the way marketers approach targeted campaigns, especially online?

Currently, technical identifiers and data (such as IP addresses or device identifiers) fall into a grey area as to whether they constitute personal information. In the case of *Privacy Commissioner v Telstra Corp Ltd*,[2] it was held that telecommunications metadata was not "about" the phone user, and was therefore not "personal information" — notwithstanding that this information could reveal information about the phone user.

The proposed change in the law is to define "personal information" as being information or opinion that "relates to" a person, as opposed to the current formulation which speaks to information or opinion "about" a person. This might seem like a lawyer's trick, but it is intended to capture a wider range of data that reveals information about an individual (such as in the case I mention above). Other practical measures are proposed in the Review Report to capture and give effect to this principle (eg, Proposals 4.1 and 4.2).

In the case of direct marketing and targeted campaigns, one approach has been to avoid privacy concerns altogether by relying upon methods that use technical identifiers, where you don't identify the individual (for example, by name). So, you may know that the user of a particular identifier has bought or browsed for product X at online retailer Y, but so long as you can't identify the person, the Privacy Act is not engaged. This is notwithstanding the fact that detailed online profiles about individuals may be built, and that it is often not too difficult to either identify a person or reduce the field of possible individuals to a very small field. I should note, for completeness, that the OAIC takes the view that this is all personal information, although I'm not aware of it having taken any public action to prosecute this point.

Under the reforms, the expansion of the scope of the definition of "personal information" coupled with new requirements around consent and opting-out of direct

marketing, will likely require marketers to treat technical identifiers in the same way that they would be required to treat other forms of personal information.

This will likely encompass data that is used to build personal profiles, notwithstanding that the usual forms of identifying information are not collected (such as names, contact information). This will also need to ensure that they have right systems in place to obtain consent (and allow individuals to opt-out) before conducting any direct marketing campaigns. Systems for these sorts of things already exist, but they may need to be reconfigured to address these changed laws.

As many readers would be aware, cookies are a device relied upon for online marketing, but which have for a long time been a cause of concern for privacy reasons. Many of the alternatives to cookies seek to avoid the "creepiness" of cookie tracking (for example, you are browsing a website and then are presented with ads from that website many days and weeks afterwards), but still rely upon some form of technical identifier. It is possible that the reforms will capture some of these technical identifiers where they enable a person to be identified.

For companies that are using third-party service providers to assist them conduct these marketing campaigns, it will be essential that they have put in place the appropriate contractual mechanisms to ensure that the Privacy Act is being complied with. The risk is that that the way the marketing is conducted puts the company in breach of the Privacy Act, notwithstanding it is the third-party service provider that is performing the actual marketing activity. It is not a defence for a company to point to a misbehaving service provider!

Q: In the context of direct marketing and transparency, Proposal 16.3 suggests enhancing the information on direct marketing in APP privacy policy. How do you see this increasing transparency impacting the trust and relationship between consumers and businesses, if at all?

Proposal 16.3 is directed at ensuring that collection notices be transparent and easily able to be understood by a child (where the relevant collection and use of personal information relates to a child). However, whether addressed to a child or an adult, it makes good business sense to ensure that privacy policies are clearly and accurately expressed.

Being clear and upfront not only demonstrates the seriousness with which a business treats their privacy responsibilities, but also reduces the risk of disputes where the business can show it took reasonable steps to bring relevant matters to individuals' attention. I know I have spoken to date about some of the increased compliance burden on companies, but, ideally, this will lead to greater trust between consumers and business with the benefits outweighing the costs involved.

One matter which the government has indicated that it agrees in principle with is the requirement of companies to undertake Privacy Impact Assessments (PIA) prior to the commencement of high-risk activities. PIA should be seen as an opportunity by business to demonstrate, publicly, their commitment to privacy-by-design and privacy protection. That is, they should not be seen as merely an exercise undertaken for compliance purposes. While these are relatively common in the public sector, they would be novel for many businesses. It will be important for lawyers and privacy practitioners to develop the skills to lead their organisations through a PIA and to demonstrate how they are beneficial to business and customer relationships.

Q: I now turn to the topic of the OAIC's Position on "influencing behaviour". I understand from one of your articles that the OAIC has pointed out that the term "influencing behaviour" is broad and could encompass various conducts. In your opinion, should there be a clearer definition or parameters set to what counts as "influencing behaviour" in the realm of direct marketing?

Over the course of the (many) discussion papers and review reports, the discussion moved away from "influencing behaviour" per se and to the concepts of "direct marketing" and "targeting". The current position is that these terms be clearly defined, with the result that greater responsibilities are placed when "targeting" is conducted.

I do think that the concept of "influencing behaviour" is, on its own, somewhat unclear as it potentially captures conduct which is not problematic. I do think it makes sense to distinguish between "direct marketing" and "targeting" as some of the mischiefs that arise when targeting takes place don't arise to the same degree in respect of what might be described as "bare" direct marketing.

However, the shift in the discussion has also meant that the focus has moved from a question as to (1) whether the influencing conduct is within the primary purpose for which the personal information was collected, to (2) whether the targeting of individuals is fair and reasonable in the circumstances. In a lot of cases, these two different tests will point to the same answer —

however, you can see how the test (2) puts less emphasise on what was done at the point of collection and asks normative questions about whether the conduct is fair and reasonable.

Q: Andrew from what I have seen, industry responses to the regulatory burden have been cautious — can you speak to the challenges businesses might face in adhering to these regulations and whether the potential benefits to individuals justify these challenges?

Business will very likely be required to redesign systems and processes to comply with these new laws. Not only are consumer expectations changing when it comes to direct marketing, but the regulator will have new powers to monitor and enforce these new laws. Quite apart from the technological and process issues that business will need to deal with are issues relating to existing data set/leads and whether the right data has already been collected to allow relevant marketing campaigns to be conducted.

Ultimately, if consumers have greater trust in respect of how businesses handle their personal information, this can only be a good thing for all parties involved. I'd also note that what is being proposed is, in many respects, consistent with what is already in place in other parts of the world, so it is not as though Australia is an outlier in that respect.

Separately, the reforms will build on the increased penalties introduced in late 2022 (maximum penalties for companies being the greater of (a) $50 million; (b) 3x value of benefit obtained from the breach; and (c) 30% of the company's turnover during the period of the breach).

To date, there has been relatively little enforcement action taken by the OAIC, as compared with other non-privacy regulators in Australia as well as privacy regulators overseas. Part of the reforms include increased funding for the OAIC (including a possible industry funding model), as well as the introduction of low and mid-tier penalty provisions. These will increase the likelihood that the OAIC will take enforcement action against companies. Regardless of whether any penalties are levied, increased action by the OAIC is likely to bring increased media scrutiny on business and the concomitant risk of reputational damage.

Q: Given that the technology and business practices have significantly evolved since APP 7 was introduced, in what ways do you believe the current proposals address these changes, and in your view, where might they still fall short in anticipating future evolutions in direct marketing?

One issue with the current APP 7 that the proposed laws don't quite address is that it makes unstated assumptions about what the form of direct marketing may take. I say unstated, because APP 7 requires the direct marketing message to include particular information which new ways of direct marketing may not be able to meet. For example, would the display of advertising to a person using an augmented reality device constitute direct marketing (assuming the person's personal information is being used) — if so, how does the company provide a "prominent statement" that the individual can opt-out? Or to pick a less futuristic example, do the notifications you receive on your phone from an app you have installed amount to direct marketing, and if so, how is APP 7 complied with?

Q: How do privacy laws intersect with marketing strategies on social media, and what legal challenges do companies face in adhering to these laws?

Very often, marketing strategies on social media will inform some form of "targeting" — that is, marketing is targeted at particular kinds of users, for example, based on their location or other interests.

One issue that companies will need to ask themselves is whether any of their marketing will be targeted at children, or at user groups that are likely to have children — new requirements requiring business to act in the best interests of the child when conducting such marketing campaigns will need to be addressed. Secondly, businesses will need to be transparent about how they conduct online marketing, including on social media. Thirdly, business will need to make sure that all necessary consents have been obtained (including that any such consents are current etc). Where third-party service providers are relied upon, then business should ensure that their arrangements with those service providers contain adequate warranties and other protections.

Q: What are the legal implications for businesses regarding the collection and use of consumer data on social media platforms, especially in light of global privacy regulations?

These risks prevail today — the extra territorial application of GDPR and other non-Australian privacy laws potentially captures conduct by Australian business where they are using the information of foreign individuals to market to those foreign individuals. Systems, processes and marketing campaigns should be designed with the potential for these foreign laws to apply specifically in mind — for example, if you are marketing specifically to the Australian market, then any marketing should reflect this (for example, you shouldn't be sending targeted marketing to users located outside of Australia). Conversely, if you are specifically targeting consumer in Europe, then there is a risk you are subject to the GDPR by virtue of this alone, and your systems and processes should be designed to address any GDPR requirements.

Q: What legal requirements exist for influencers and brands in terms of disclosing sponsored content on social media to ensure consumer transparency?

Sponsored consent on social media falls under the same rules as other kinds of advertising. This isn't a privacy issue per se, but it is a consumer protection issue. This means that the content of the posts must be truthful (and not misleading or deceptive). It also means that any sponsorship should be disclosed — the way that consumers are likely to interact with a sponsored vs non-sponsored post is different, and so consumers are likely to be misled if sponsorship is not disclosed.

Q: When using user-generated content in social media marketing, what are the key legal considerations related to privacy?

The key privacy considerations relate to the privacy of the relevant user who generated the content, as well as the privacy of any individuals in the content itself.

The fact that the content may otherwise be publicly available will not absolve a business from their obligations under the Privacy Act if they then use that information. You should remember that personal information, as defined in the Privacy Act, may include confidential as well as non-confidential information!

Q: As social media platforms introduce new features (like augmented reality), what changes in public policy might be necessary to address privacy and marketing, and how should businesses prepare for these changes?

The challenge for regulators is an age-old one — how to keep laws up to date to reflect current technology and ways of doing business. Proposals such as Proposal 11.2 go some way in empowering the OAIC to provide guidance for business in respect of how consent is obtained online — although your question clearly speaks to issues much broader than mere consent. Your augmented reality example is a good one, and highlights the difficulty in applying current laws.

For example, if marketing materials communicated over augmented reality amounted to a form of direct marketing (which is entirely conceivable), then how would that communication meet the requirements of APP 7 — for example, to include a statement that the individual may opt-out of that marketing? Businesses that seek to understand and implement tools and measures that reflect both the letter and spirit of the law will be best placed to deal with these changes — we see that already today, with many of the additional privacy measures offered on a number of different technology platforms being driven not because of legal compliance reasons, but rather to meet the demands of consumers.

Andrew Hii
Partner
Gilbert + Tobin
AHii@gtlaw.com.au
www.gtlaw.com.au

Sharon Givoni
Principal
Sharon Givoni Consulting
sharon@iplegal.com.au
www.sharongivoni.com.au

Footnotes

1. Attorney-General Department *Privacy Act Review* Report (2022) www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf.
2. *Privacy Commissioner v Telstra Corp Ltd* (2017) 249 FCR 24; (2017) 347 ALR 1; [2017] FCAFC 4; BC201700165.

Targeted advertising and profiling — charting a new course in Australian privacy law and regulation

Peter Leonard *DATA SYNERGIES AND UNSW BUSINESS SCHOOL*

Design of sensible and proportionate reforms to provisions of the Privacy Act 1988 (Cth) to regulate targeted advertising and profiling requires careful consideration of:

- how targeted advertising and consumer profiling may be used in ways that cause privacy harms to individuals
- how risks of these harms can be mitigated through adoption of responsible data practices
- how the Australian Privacy Act might create the right incentives for responsible data practices and ensure strong disincentives for failures to properly control collection, use and sharing of data for targeted advertising and profiling

This short paper addresses these design requirements. We first discuss relevant concerns often expressed about targeted advertising and profiling, before examining how those terms are variously used, and current and proposed regulation.

Getting our terminology straight

"Online targeted advertising" uses data analyses of information related to a person's activities online, either in a particular internet session (contextual advertising) or combined with information about a person's previous activities online or offline information relation to that person or "lookalikes" (inferred to be similar persons), to classify a person as within a specific audience or segment for delivery of an online advertisement to that audience or segment but not to others. The main benefit of targeted advertising to advertisers and individuals is that ads displayed to individuals will be more relevant and personalised.

Targeted advertising may use only information related to a person's activities collected by one party or with consent by related parties (ie, program partners in loyalty program, often called "first-party data", or may be combined with information related to a person's activities sourced from third party, often called third-party data. Sometimes data intermediaries make available third-party data — entities conducting such activities would generally be regarded as data brokers, although some privacy advocates use that term to describe any entity sharing any information related to a person's activities with any third party.

Online targeted advertising is a subset of "targeting" or "microtargeting" — these terms are often used interchangeably. Targeting may determine what and how relevant content is delivered to an individual online. Targeting is generally used to market products or services, including (and more controversially) for political marketing (ie, if you are inferred likely to follow a certain political party or ideology on a social media platform, personalised ads related to that party or ideology may be displayed to you).

The ability to deliver advertising to audiences likely to be interested in those products translates into monetary value for media publishers (ie, internet sites that may or may not be making available news of other traditional media content) that make available digital advertising canvas into which digital ads may be inserted), digital platforms (ie, Google, Meta, Apple and Amazon) that deliver users to those internet sites or themselves host or provide content, and myriad adtech intermediaries that make this multiparty digital advertising ecosystem work.

Data analysis for online targeted advertising may, or may not, use information that is personal information about or relating to individuals, depending upon the design of the data environments and specification of adtech technologies and associated data flows associated with creation and use of the audience or segment used to target the online advertisement. The last sentence states the most misunderstood aspect of online targeted advertising — this misunderstanding is common across many lawyers, policymakers, media and consumer and privacy organisations. It is possible, and increasingly common, for online targeted advertising to be conducted using information relating to an unidentified transactor's activities that is not personal information about or relating to an individual. This paper endeavours to explain how to avoid that misunderstanding and thereby design sensible regulation.

"Profiling" refers to collection and use of information, either known information or inferences, as to attributes, characteristics, preferences or activities of individuals, whether or not those individuals are identified or reasonably identifiable. Profiling as such is a normal part of everyday activities of almost every organisation (including government agencies and charities and political parties) nowadays — customer relationship management (CRM) and supplier relationship management (SRM) databases typically include profiling data. Profiling data may or may not be used to tailor offers (which may be non-advertised offers) or determine a manner of differential treatment of those individuals having regard to their attributes, characteristics, preferences or activities. Profiling may, or may not, be used for targeting, or for the subset of targeting that is online targeted advertising. Use of profiling data for targeting may be for online marketing, commercial electronic messages, direct marketing and human-to-human (call centre, or face-to-face) interactions. Use of profiling data for targeting may or may not involve use or disclosure of personal information about or relating to individuals — each use case and the data context of that use case must be evaluated.

Concerns as to targeted advertising and profiling

Targeted advertising and profiling practices are increasingly contentious. There is contention as to which practices should be regulated and how. There is contention, and often confusion, as to which entities are now doing what, and how.

Consumer data advocates and privacy professionals' express concerns that some Australian Privacy Principle (APP) entities engage in targeted advertising practices that are excessive (beyond those reasonably necessary for one or more of the entity's functions or activities, and thereby contravene APP 3.2), unexplained or poorly explained, not transparent, or only "allowed" through use of "dark patterns" (deceptive choice architecture) which undermine exercise of choice and control by affected individuals.[1]

Expressed concerns often focus upon targeted advertising where activities and movements of individuals are tracked across multiple devices (so-called "cross-context tracking"), over time and across multiple online sessions and in some use cases in conjunction with geolocation tracking.

Sometimes expressions of concerns centre upon uses of user data through linking with transaction data such as credit and debit card or loyalty card data — a linkage which can enable measurement and attribution of whether and how tracked users respond through purchases to targeting "calls to action".

By contrast, some APP entities that use or facilitate targeted advertising point to their adoption of data clean rooms and privacy enhancing technologies as a means of ensuring that non-consented personal information is not used for targeted advertising, and as a means of creation of aggregated or fully anonymised insights for organisations as to their customer or user base.

Some APP entities dispute allegations that their data practices associated with advertising and customer analytics do not comply with existing provisions of the Australian Privacy Act, and allegations that their descriptions of data practices are misleading and contravene the Australian Consumer Law (ACL).

The global policy debate about targeted advertising and profiling

Debates as to appropriate coverage and regulatory settings for targeted advertising and profiling are currently active in many jurisdictions. There are varying statements of the problem to be solved, and accordingly a range of proposals for new rules.

In many jurisdictions, the regulatory focus has been upon addressing online targeted advertising enabled through use of pervasive tracking codes such as cookies, pixels and device identifiers. Regulators have cited examples of poor data practices of some digital advertisers and adtech providers that share tracking codes and device identifiers or enable correlation of multiple codes and device identifiers that are inferred likely associated with a unique transactor. Regulators have also cited examples of digital advertisers and adtech providers that fail to control uses of user data within multiparty data ecosystems in which they participate. Failures of control demonstrate a lack of responsibility and accountability of relevant data controllers. These failures may lead to outcomes where other parties within that data ecosystem use and disclose user data inconsistently with privacy collection notices and other statements made by the advertiser or provider, and otherwise breach data privacy law.

There has been less active debate about whether, and if so, how, to address practices in targeting outside of the subset of online targeted advertising.

In other words, global regulatory reform discussions have generally focussed upon online targeted advertising, as "advertising" is commonly understood, and not the myriad other ways in with businesses, government agencies and other organisations elect to profile and differentiate between consumers and users, having regard to individual attributes, etc. These differentiations are increasingly data and algorithmically informed and commonly enabled by technological automation.

Automated decision making (ADM) and AI

Historically, differentiation between consumers (short of legally prohibited discrimination) took many forms. Those forms included a street vendor determining the price of oranges based upon a visual evaluation of a prospective customer's dress and demeanor and the vendor's quick inference (heuristic) as to that customer's capacity and willingness to pay. Digital data, algorithmic inferences and online interactions now enable differentiation between individuals at speed and efficiency.

Associated with public interest and rapid uptake of open large language models (LLMs) and generative AI (GenAI) over the last 12 months, policy makers are expressing concerns as to how emerging AI capabilities will enhance ability of organisations to differentiate at increasing speed, efficiency and granularity. This is leading policy makers, legislatures and regulators to reevaluate whether data privacy statutes are adequate and sufficient, or whether consumer protection or AI-specific laws should supplement privacy regulation.

ADM has led to topic-specific regulatory responses, such as EU's General Data Protection Regulation (GDPR) Art 22 (Automated individual decision-making, including profiling).[2] A broadly analogous rule now proposed by the Australian government would require privacy policies to set out the types of personal information that will be used in substantially automated decisions which have a legal, or similarly significant effect on an individual's rights.

The government also proposes to confer upon individuals a right to request meaningful information about how automated decisions with legal or similarly significant effect are made, to be provided by an APP entity in a "jargon-free and comprehensible" form.[3]

California to lead the way?

One possible future in regulation of targeting and profiling is a current (as of March 2024) proposal by the California Privacy Protection Agency for new rules under the California Consumer Privacy Act 2018 (CCPA).[4]

This proposal includes:

- an expanded (from the current CCPA provision) definition of "profiling", as any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's intelligence, ability, aptitude, performance at work, economic situation; health, including mental health; personal preferences, interests, reliability, predispositions, behavior, location, or movements
- a new definition of "behavioral advertising", as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity — both across businesses, distinctly-branded websites, applications, or services, and within the business's own distinctly-branded websites, applications, or services. The proposed definition also expressly includes "cross-context behavioral advertising", and excludes "nonpersonalized advertising, provided that the consumer's personal information is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business, and is not disclosed to a third party
- regulation of behavioral advertising as so defined as a form of "extensive profiling" and therefore also within a definition of "automated decision-making . . . that has a significant impact on consumers", then requiring provision of a complex notice in advance as to the practice, and provision of ability for consumers to opt-out

Extension of enhanced notice and opt-out requirements

This proposed new rule would overlap with enhanced notice and opt-out requirements already in place in California under CCPA, that apply to "sharing" of "personal information" for "cross-context behavioral advertising". Use of personal information from more than one party — eg, cross-site/app/service browsing information, or combinations of first-party data and third-party data — is currently in-scope for enhanced notice and opt-out requirements under the CCPA. The new rule would in effect make "cross-context behavioral advertising" a subset of newly defined "behavioral advertising". This would bring within the scope of CCPA requirements for enhanced notice and opt-out any practice that involves the use of personal information, even exclusively first-party data, for targeted advertising, but with limited exceptions that would include where the advertising is based solely on a current interaction (eg, contextual advertising).

The Californian proposal goes significantly beyond data privacy statutes in other states of the USA,[5] the current scope of EU GDPR and UK GDPR, and provisions of data privacy statutes in highly regulated jurisdictions such as Japan and Korea.

How do Australian reform proposals compare with the Californian proposal?

What the Australian Government proposes

The Australian Government Privacy Reform Proposal states that amendments to the Privacy Act are needed to clarify that personal information is an expansive concept "that includes technical and inferred information, such

as IP addresses and device identifiers, if this information can be used to identify individuals".[6]

The Government states that an individual may be reasonably identifiable where they are able to be distinguished from all others, even if their identity is not known.

> This will require consideration of whether the information available — whether by itself or in conjunction with other information available to the entity — is sufficient to be linked to a particular individual even if their name is not known, or if there is a reasonable likelihood of identification or re-identification of an individual (that is, whenever the risk of identification or re-identification is higher than low or remote). For example, if a website publisher uses persistent cookies, device fingerprinting, or similar unique identifiers, the publisher may be able to identify a visitor, even if the visitor's IP address is not unique to that visitor.[7]

The Government also proposes that the definition of "deidentified" is:

> . . . amended to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.[8]

New categories for regulation

The Government "accepts in principle" that as well as continued regulation of direct marketing, the Act should regulate:

- "trading", being "the disclosure of personal information for a benefit, service or advantage"
- "targeting", being:

  > . . . collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc) 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).[9]

As well as more specific and higher regulation of targeting to a child and as to uses of geolocation data collected over time, and a prohibition upon trading of personal information without express consent, the Government proposes to provide individuals with "an unqualified right to opt-out of receiving targeted advertising".

"Targeting" rules with broader scope than "targeted advertising"

The proposal for an opt-out is specific to "targeted advertising", and therefore does not apply to other forms of "targeting" such as non-advertised segmented or differentiated offers enabled through creation and use of profiling.

However, "targeting" uses of profiling, as well as targeted advertising, would be regulated by new rules including the following:

- Targeting individuals must be objectively fair and reasonable in the circumstances, regardless of consent.
- Targeting individuals based on sensitive information would be prohibited, with an exception for socially beneficial content.
- APP entities would be required to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals.[10]

Open questions

It remains unclear how the Government proposes that the amended Act would address non-advertising targeting through collection, use or disclosure of information which relates to an individual, but which is not personal information, being "deidentified information" or "unidentified information (internet history/tracking etc)", "for tailoring services, content, information . . . or offers provided to or withheld from an individual (either on their own, or as a member of some group or class)".[11] Many services and offers of features within services today are targeted through creation and use of inclusion or exclusion audiences, and sometimes are so targeted in order to meet legal requirements (for example, for a financial services licensee not to offer financial products to a class of consumers where that class might reasonably be anticipated to suffer financial hardship were they to take up that offer).[12]

Further, the Act today only regulates uses of personal information about an individual. The Government proposes to extend the definition of personal information to include information relating to an individual, while retaining the concept of reasonably identifiable individual[13]. Key questions arise:

- If regulation of "targeting" is specifically extended to include uses of deidentified information relating to individuals and "unidentified information relating to" individuals, how should "relating to" be interpreted?
- Is extension to uses of deidentified information and unidentified information intended to include targeting use of any inference as to attributes, characteristics, preferences or activities of an unidentified transactor that is derived from data about that unidentified transactor, and thereby including contextual differentiated offers, as well as contextual advertising?
- If so, what is the nature and extent of "information about targeting", including (and therefore not

limited to) "clear information about the use of algorithms and profiling to recommend content to individuals", that must be provided by an APP entity in order to satisfy the new transparency obligation?

The way that these questions are addressed through legislative drafting and associated regulatory guidance will fundamentally reshape the myriad ways in which targeting and profiling takes place today across all sectors of the Australian economy, and not just targeted advertising and the online digital advertising sector.

If the Australian Privacy Act is amended consistently with these proposals, uses of consumer profiling in Australia by all APP entities will become more highly regulated than in comparable data privacy regulating jurisdictions, including the EU, California, Japan and Korea.

The scope and operation of the Australian Privacy Act in relation to consumer profiling will also fundamentally change from current provisions.

The following section examines how the provisions of the Australian Privacy Act currently operate in relation to targeted advertising and consumer profiling.

How the Privacy Act operates today

The Australian Privacy Act regulates acts and practices of APP entities in collection and handling (use and disclosure) of datasets containing personal information. Personal information is "deidentified" "if the information is no longer about an identifiable individual or an individual who is reasonably identifiable", whether or not those individuals are specifically identified (ie, named) in the data set.[14] "Reasonably identifiable" is not defined, but the term has been the subject of multiple Office of the Australian Information Commissioner (OAIC) guidance materials for many years.[15] The substance of that guidance is broadly comparable to regulatory guidance as to EU GDPR and UK GDPR and, in the view of the writer, not contended. Individuals may be reasonably identifiable from the relevant data sets themselves, or through reference to other information that is reasonably available — the data context of the entity handling the data must be considered.

Broadly (and subject to various statutory exceptions), there are two possible bases for handling of personal information regulated by the Australian Privacy Act:

- fully transparent disclosure to affected individuals, including obtaining their consent where and to the extent that consent is expressly required by the Australian Privacy Act in relation to particular types of data (ie, sensitive personal information), or particular regulated acts or practices
- deidentification of relevant information, so it no longer is required to be handled as personal information, while in that particular data context

Consistent with current OAIC guidance as to interpretation of the Australian Privacy Act, an APP entity is considered to only handle "deidentified information" where in the data context(s) in which that information is collected and handled by that APP entity, the risk of reidentification of individuals is "very low".[16] The Government Privacy Reform Proposal uses an alternative form of words, namely that the Government considers that individual may be reasonably identifiable "wherever the risk of identification or reidentification is higher than low or remote".[17] It is not clear to this author whether any practical distinction can be reliably drawn between "very low" and "low or remote" — a matter of practical privacy risk assessment and mitigation, there is not a significant distinction between these phrases.

Self-collection through inference

The current provisions of the Privacy Act regulate, as "personal information", information about an individual, in contradistinction to information that relates to an individual. The Government Privacy Reform Proposal includes a proposal to amend the Privacy Act to include (within the scope of regulated personal information) information that "relates to" a reasonably identifiable individual.[18] For many information types and data contexts, a practical distinction can be made between information about an individual and information that relates to an individual. However, in the particular context of targeted advertising and profiling of individuals, the distinction may not be significant, insofar as each phrase is used in respect of a reasonably identifiable individual. Information inferred from browsing activity or transactions is often information as to attributes, characteristics, preferences or activities of that transactor.

The making of an inference about a transactor that is derived from analysis of data to infer attributes, characteristics, preferences or activities of that transactor could be argued to not be a collection of information, as "collection" is currently defined and used in the Privacy Act. However, that argument is legally weak, and in any event any such argument is likely to be foreclosed by the proposed reforms.[19] In the writer's view, if the context of use of inferred information is provision of targeted advertising or other targeted content to a transactor that has been selected having regard to inferred attributes etc, of that transactor, whether individually or as a member of a group or segment of individuals inferred to share inferred attributes etc, this use of inferences would appear to be a use of inferred information that is both about and relating to that individual.

Data context — when is there a handling of personal information?

A more difficult and contested question then arises — whether and when an act or practice of targeted advertising or profiling of an individual involves a collection or use or disclosure of personal information (regardless of whether about or relating to that individual).

A transactor may be tracked or profiled over time and across transactions, and across devices (cross-contextually), through use of a transactor code or key (ie, without the individual transactor being identified by name or other direct identifier), or through use of cookies, pixels or other tracking code associated with a browser, or device or SIM numbers, or through use of a loyalty card or membership number allocated to that (otherwise not directly identified) transactor.

As many privacy advocates correctly observe, in many data contexts to date those transactor codes or keys could readily be re-associated or linked back to an identifiable individual, whether through look-up or association tables that facilitate such identification (or reidentification), by some participants in multiparty data ecosystems within which information associated with those transactor codes or keys are made available. Often to date cookies, pixels or other tracking codes or fingerprints have been associated with browser applications in circumstances where the transactor using that browser could be reasonably identifiable by some entities that have access to that tracking code or fingerprint and information associated with it, and therefore that associated information is personal information in relation to those (thereby identifiable transactors) when in the hands of those entities, applying current provisions of the Privacy Act. It is their capability to identify (or reidentify) the relevant transactor, and not their intent or actual practice, that is legally relevant.

An APP entity's data architecture and data handling processes and practices, both technical and operational, and associated legal (including contractual) arrangements, taken together determine the data context in which that entity collects and handles relevant data.

In many data contexts to date, identification risks are not appropriately assessed and mitigated. For example, mosaic or pattern analysis of information associated with that transactor code or key may facilitate identification of a transactor.

To take but one example, geolocation tracks of mobile devices over time may point to a common evening address and likely work address of an otherwise deidentified transactor, unless start and end points and localities are sufficiently obfuscated. If an APP entity operates a data environment handling "on the face of the data" deidentified information in circumstances (a data context) where the risk of mosaic or pattern reidentification of transactors associated with transaction or transactor data is greater than low or remote, that entity is likely to be handling personal information. (The separate question remains as to whether that information is about an identifiable individual and therefore captured by the Privacy Act as it currently stands, or relating to that identifiable individual and therefore only captured if the Act is amended as proposed by the Federal Government.)

Data context changes when data, whether in the form of release data, insights, reports or other outputs, passes from one controlled environment into other controlled or uncontrolled environments. Assessment of reidentification risk at point of release should be made in the particular data context of each release, having regard to any conditions imposed upon a recipient, including contractual restrictions imposed upon a recipient as to downstream disclosures or subsequent uses, and capabilities of a recipient to identify relevant transactors. This assessment should also consider the level of risk that:

- these conditions may not be complied with
- operation of these conditions may be circumvented by exfiltration of release data as may be instigated by a motivated intruder

Risky multiparty data ecosystems

If a transactor key or code is made available in a data environment that is not adequately protected against look-up or association of that key or code with identifiers of an individual, or data within that data environment is not safeguarded against identification or reidentification analysis by persons (including malicious external actors) able to access data within that data environment, the information should be regarded as personal information, because some individuals within the relevant datasets may be reasonably identifiable.

Often entities fail to take adequate steps to secure and safeguard multiparty data ecosystems within which those entities share information associated with transactor codes or keys, and as a result that information should be regarded as uncontrolled and therefore potentially personal information.

This may be the case even though the entity may not intend the information within that multiparty data ecosystem to be used by any party for identification of an individual and may have contractually prohibited use of information for that purpose.

It is the absence of verifiably reliable technical, operational and legal (including contractual) safeguards and controls in this data context that leads to the information being information about or relating to reasonably identifiable individuals and therefore personal information.

Legal contentions

Three associated questions often arise in relation to creation of inferences for the purpose of targeted advertising or profiling through use of information associated with transactor codes or keys of unidentified transactors, rather than associated with direct identifiers of individuals.

The first question arises where information is treated before analysis to remove identifying information about individuals. Is that act or practice of deidentifying treatment itself a regulated use of personal information, because the information before treatment is reasonably identifying information about an individual?

The commonly accepted legal view is that it is not a regulated use — deidentification may be by many means, including by aggregation and obfuscation of direct identifiers. On this view (and noting that some privacy advocates dispute the following legal analysis), the Act as it stands does not regulate deidentified information if conducted such that the residual risk of reidentification of a relevant individual in the particular data context is objectively low or remote. This is sometimes called deidentification to the level of "effective anonymisation", to distinguish this level from "pervasive anonymisation" where even remote risk of reidentification is removed.

The second question is whether APP 3.5 relevantly operates.

APP 3.5 provides that "an APP entity must collect personal information only by lawful and fair means". APP 3.5 could be activated through self-collection by inference, but only where the inference is self-collected by an APP entity or on its behalf in a data context where the information so collected is about a reasonably identifiable individual. If the data environment in which that inference is created is safeguarded and controlled in the manner above described, there should not be a relevant collection or handling of personal information within that data context.

The third question is whether APP 3.6 relevantly operates.

APP 3.6(b) provides that an APP (non-government) entity must collect personal information about an individual "only from the individual . . . unless it is unreasonable or impracticable to do so". Some privacy lawyers have argued that targeted advertising and consumer profiling facilitated through analysis of activities etc of particular unidentified transactors is a collection of information about those individuals other than directly from those individuals in contravention of APP 3.6.[20] In the writer's view, a similar analysis applies to APP 3.6 as to APP 3.5 — APP 3.6 may be activated through self-collection by inference, but only where the inference is self-collected in a data context where the information so collected is about a reasonably identifiable individual.

Beware the gap: ACL

The above analysis relates only to the operation of the Australian Privacy Act. Some organisations engaged in targeted advertising or consumer profiling contravene ACL by making statements as to what they "only" do with "personal information" or "your information", or as to what those organisations "don't do" with information "about you" or "consumer data", that in the context of the targeted advertising or consumer profiling are misleading or deceptive.[21]

In many cases of consumer concern as to excessive, unreasonable or unreasonably opaque targeted advertising or consumer profiling, these concerns could be addressed through rigorous application of the ACL prohibitions on misleading and deceptive statements.[22] By way of comparison, the US Federal Trade Commission (FTC) exercises its deceptive business practices jurisdiction[23] to be the highest fining data privacy regulator globally (far exceeding EU and the UK), notwithstanding absence of a federal data privacy statute in the USA.[24]

Anonymisation-based targeted advertising and consumer profiling is technically and operationally complex to implement and also difficult to explain to consumers in terms that are transparent and understandable and not misleading. It is now commonplace for an organisation to be "hoist on its own petard" of statements made somewhere on its website, or elsewhere in its marketing and customer communications, that are misleading by omission of material particulars or qualifications. One enforcement priority of the US FTC has been to curtail the widespread availability and use of consumer information for consumer profiling, including through activities of data brokers, in circumstances where the entities making available that information have made statements directly contradicted by their activities.[25]

Accountability for downstream activities and entities

A further complexity in privacy compliance for APP entities engaging in targeted advertising or consumer profiling is that downstream activities of those entities, or of other entities in relation to whom they are legally accountable, may constitute a contravention.

For example, marketers often seek validation of their expense and effort in buying media canvas for targeted advertisements or in curation and provision of targeted content through measurement of whether and how a particular transactor responded to the "call to action"

constituted by that targeting. Measurement requires attribution, and any individual level attribution may itself be a collection and use of personal information about an individual.

Further, many entities seek to augment their consumer (customer) relationship management databases by addition of "customer behavioural factors" or attribute information about known individuals, including attributes derived through anonymisation based analysis of information about unidentified transactors.

Provision of individual level attribute information relating to particular individuals that are identifiable in the hands of the recipient, whether or not derived from anonymisation based analysis of information about individual transactors, is likely to be either or both a disclosure of personal information or a collection by a recipient APP entity of further personal information about known individuals.

Provision of aggregated insights as to effectiveness of calls to action may not involve disclosure or collection of personal information.

Many organisations today do not properly evaluate and control the form of outputs that they release from controlled data environments, and as a result handle regulated personal information.

Conclusion

Targeted advertising and profiling practices are increasingly contentious, as to which practices should be regulated and how, and contented, as to which entities are doing what and how.

Debates as to appropriate coverage and regulatory settings for targeted advertising and profiling are currently underway in many jurisdictions. There are varying statements of the problem to be solved, and accordingly a range of proposals for new rules across various jurisdictions.

There has been less discussion as to uses whether and how to address practices in consumer profiling outside of online targeted advertising, and in particular offline marketing applications of consumer profiling.

The global highwater mark of developed proposals for regulation of targeting using personal information is the current (as of March 2024) proposal by the California Privacy Protection Agency for new rules under the CCPA. That proposal goes significantly beyond data privacy statutes in other states of the USA, the current scope of EU GDPR and UK GDPR, and provisions of data privacy statutes in highly regulated jurisdictions such as Japan and Korea.

The less developed (still in outline) Australian Government Privacy Reform Proposal is that the Australian Privacy Act is amended to go further again, to regulate (as well as targeted advertising facilitated through use of personal information) non-advertising targeting facilitated through collection, use or disclosure of "deidentified information" or "unidentified information (internet history/tracking etc)" relating to individuals.

It is currently unclear what is intended scope of coverage of this proposal.

However, the outlined scope of coverage does appear to be substantially broader than more developed proposals in comparable jurisdictions, including the global highwater mark of California.

The way that these questions are addressed in Australia through legislative drafting and associated regulatory guidance will fundamentally reshape the myriad ways in which targeting and profiling takes place today across all sectors of the Australian economy, and not just targeted advertising and the online digital advertising sector.

Marketing and data science professionals, as well as lawyers, need to be engaged in discussions with policymakers, in order to ensure that when Australia fundamentally changes provisions of the Australian Privacy Act, the new settings as to targeting and profiling address irresponsible and excessive practices, but do not preclude fair and reasonable targeting and profiling.

About the author

Peter Leonard is a business consultant and lawyer advising data-driven businesses and government agencies. Peter is principal of Data Synergies and a part-time Professor of Practice at UNSW Business School. Peter serves on the OECD Expert Group on AI, Data, and Privacy, the Australian National Data Advisory Council, the NSW Government's AI Review Committee, the Data Standards Advisory Committee and a number of corporate and advisory boards. Copyright © 2024 Data Synergies Pty Ltd.

Peter Leonard
Principal, Data Synergies Pty Ltd
Professor of Practice, UNSW Business School
pleonard@datasynergies.com.au
www.business.unsw.edu.au

Footnotes

1. For example, see W Christl and A Toner *Pervasive identity surveillance for marketing purposes* Report (2024) https://crackedlabs.org/en/identity-surveillance; K Manwaring, K Kemp and R Nicholls *(mis)Informed Consent in Australia* UNSWorks Report (2021) https://dx.doi.org/10.2139/ssrn.3859848; K Kemp "'A rose by any other unique identifier': Regulating consumer data tracking and anonymisation claims" *Competition Policy*

International TechREG Chronicle 18 October 2022, pp 21–29 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4248453; K Kemp, C Gupta and M Campbell *Singled out — Consumer understanding — and misunderstanding — of data broking, data privacy, and what it means for them* Report (2024) https://cprc.org.au/report/singled-out; Consumer Policy Research Centre *Not a Fair Trade — Consumer views on how businesses use their data* Report (2023) https://cprc.org.au/not-a-fair-trade. As to the current operation of Australian Consumer Law (ACL) in relation to so-called "dark patterns", see M Camp "Skippers, Skimmers and Readers: Australian Competition and Consumer Commission v Google LLLC (No 2)" (2023) 31 *AJCCL* 143; *Australian Competition and Consumer Commission (ACCC) v Google LLC (No 2)* [2022] FCA 1476; BC202217321. As to dark patterns generally, see UK ICO and UK CMA *Harmful Design in Digital Markets* Report (2023) www.drcf.org.uk/__data/assets/pdf_file/0024/266226/Harmful-Design-in-Digital-Markets-ICO-CMA-joint-position-paper.pdf; OECD *Dark Commercial Patterns* OECD Digital Economy Papers No 336 (2022) www.oecd.org/digital/dark-commercial-patterns-44f5e846-en.htm.

2. See https://gdpr-info.eu/art-22-gdpr/.
3. Attorney-General's Department *Government Response to the Privacy Act Review Report* (Government Privacy Reform Proposal) (2024) 11 www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report.
4. See Agenda and Meeting Materials for 8 March 2024 meeting of the California Privacy Protection Agency, available at https://cppa.ca.gov/meetings/materials/20240308.html. The meeting materials include a marked-up version of the California Privacy Protection Act (CCPA) that shows how the proposals would be enacted.
5. See further, A Friel and K Fath "The Problems in Calif. Draft Behavioral Ad Privacy Regs" *Law360* 7 March 2024 www.privacyworld.blog/2024/03/california-considers-restricting-broad-swath-of-content-personalization-and-online-advertising-activities/.
6. See above n 3, at 5.
7. Above.
8. Above n 3, at 15.
9. Above n 3, at 11–12 and 32 (Proposal 20.1).
10. Above.
11. Above n 3, at 32.
12. For example, see Australian Energy Regulator "Origin penalised $17 million for customer hardship breaches" media release (29 June 2022) www.aer.gov.au/news/articles/news-releases/origin-penalised-17-million-customer-hardship-breaches.
13. See further, Office of the Australian Information Commissioner (OAIC), What is personal information?, www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information.
14. See definition of "deidentified" in s 6.
15. Including OAIC, Australian Privacy Principles guidelines, Chapter B: key concepts, www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts.
16. OAIC *De-identification and the Privacy Act* (2018) 13 www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-and-the-privacy-act; see also Submission by the OAIC to The Privacy Act Review — Issues Paper, 11 December 2020, p 34 (para 2.39); Submission by the OAIC to The Privacy Act Review — Discussion Paper, 23 December 2021, p 37–38, particularly at para 2.51:

    > Under the current framework, information will be de-identified where the risk of an individual being re-identified in the data is very low in the relevant context in which it is held or released.

17. Above n 3, at 5.
18. Above n 3, at 21 (referring to Proposal 4.1).
19. Above n 3, Proposal 4.3: Amend the definition of "collection" to expressly cover information obtained from any source and by any means, including inferred or generated information.
20. Eg, K Kemp "Australia's Forgotten Privacy Principle: Why Common 'Enrichment' of Customer Data for Profiling and Targeting is Unlawful" *UNSW Law Research Paper* 20 September 2022 https://dx.doi.org/10.2139/ssrn.4224653.
21. K Manwaring "Will Emerging Information Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation" (2018) 26 *Competition and Consumer Law Journal* 141–81.
22. In particular, s 18(1) of the Australian Consumer Law (ACL), which provides that "a person must not, in trade or commerce, engage in conduct that is misleading or deceptive or likely to mislead or deceive". For application, see Australian Competition and Consumer Commission (ACCC), False or misleading claims, www.accc.gov.au/consumers/advertising-and-promotions/false-or-misleading-claims. As to enforcement, see for example ACCC "Google LLC to pay $60 million for misleading representations" media release (12 August 2022) www.accc.gov.au/media-release/google-llc-to-pay-60-million-for-misleading-representations; *Australian Competition and Consumer Commission (ACCC) v Google LLC (No 4)* [2022] FCA 942; BC202207727.
23. Section5 of the Federal Trade Commission Act (15 USC 45) prohibits "unfair or deceptive acts or practices in or affecting commerce".
24. The total amount of publicized data privacy-related fines, penalties, and settlements exacted in the US since 1999 was US$11.9 billion, exceeding any other jurisdiction worldwide, including collective enforcement across the EU of EU GDPR. This includes the FTC's $5b fine of a social media company in 2019, and a 2017 $700m action against a US financial-services firm for a widespread data breach. Taking out these large amounts, the figure is US$6.2b, of which the FTC was responsible for US$3.1b.

25. For a recent example, see L Fair "FTC says Avast promised privacy, but pirated consumers' data for treasure" *Federal Trade Commission Business Blog* 22 February 2024 www.ftc.gov/business-guidance/blog/2024/02/ftc-says-avast-promised-privacy-pirated-consumers-data-treasure; and the proposed consent order at www.ftc.gov/legal-library/browse/cases-proceedings/2023033-avast.

"No junk mail" — a privacy-first/first-party data approach to digital marketing

Alec Christie *CLYDE & CO*

Marketing and privacy (and the relevant teams within an organisation responsible for each) are often seen as "natural enemies". That is, each of their reasons for being and goals have traditionally been, and in many quarters still are, considered antithetical. Experience assisting clients with their privacy strategy, compliance and implementation over a number of years confirms this view — it is often the marketing team that puts up the stiffest resistance to any privacy compliance uplift, especially in areas that impact their existing marketing practices. Marketing teams are not opposed to privacy compliance per se — it's just that there is a perception that privacy considerations "get in the way" of their existing practices and make marketing campaigns "unnecessarily" difficult.

However, over the last couple of years globally and in the last 6 to 12 months in Australia, we are starting to see the beginnings of a fundamental shift in thinking in digital marketing. Underpinned by a "quality over quantity" strategy, marketing departments, firms and commentators are starting to appreciate that:

- privacy developments, including fines and community attitudes, have reached a point that privacy can no longer be ignored (or, at least, marginalised) and
- a focus on privacy in digital marketing can actually improve trust between an organisation and its customers/individuals which helps enhance the quality or "stickiness" of the data relationship and the success or "hit" rate of relevant marketing

A review of recent global digital marketing-focussed articles shows (and a search using your generative AI of choice will show) that these approaches are being widely discussed, often referred to as "privacy-first" and "first-party data" approaches and sometimes collectively included under the "customer-centric approach to marketing" umbrella. The virtues of these two approaches to digital marketing are being extolled by McKinsey & Company and other leading business advisory firms as a way to overcome the various recent platform and regulatory changes impacting digital marketing, such as the increasing limits being imposed on the collection and use of personalised customer data and the declining results from unfocussed, random and unwanted marketing. A core rationale of these approaches is to enable marketing to adapt to the new digital environment created by the recent moves by Apple, Google and others to reduce third-party access to and independent use of various technologies (eg, cookies, at the most basic level) and the resulting personalised information.

Why is there a need to change what you are doing now?

Of course, all marketers will be aware of the significant changes over the last decade and a half as regards the ways that personalised customer data can be gathered, used and is regulated in the digital environment. Web cookies (invented over 30 years ago in 1994 to enhance the user experience of the internet) and tracking tools such as Apple's Identifier for Advertisers (IDFA) (launched in 2012) opened the door for significant advancements in the sophistication and personalisation of marketing, profiling and targeting. The proliferation of personal information available from these tools has however also enabled third parties to take advantage of this data for their own marketing and, in some cases, for more nefarious purposes.

These developments in digital marketing have also allowed extensive privacy violations (whether or not intentional) especially where privacy laws have started to focus their attention on and imposed limits on the profiling and targeting of individuals for marketing purposes (eg, in the General Data Protection Regulation and California's Consumer Privacy Act). Further, the traditionally restrictive privacy regimes in key markets (such as Europe and California) continue to place ever more restrictive limits on the collection, use and disclosure of personal information for marketing and consumer profiling. In Australia recently, there has been a renewed focus on the use of (especially third-party collected) personal information for personalised marketing and profiling under our existing Australian Privacy Principles (APPs). Specifically, all of these privacy obligation uplifts (even in Australia) are increasingly targeting (no pun intended) those providing the tools to do this (eg, the platforms).

Commercially, the tide has continued to turn and, as of January 2024, Google began the process of phasing out support for third-party cookies in Chrome, with complete retirement to be effected in the second half of 2024. As the third browser to make this restriction, this means that approximately 85% of the browser market currently blocks (or soon will block) third-party cookies. Apple has also limited the sharing of digital identifiers with intelligent tracking prevention in Safari and the IDFA has required users to expressly opt-in to let advertisers see their data since April 2021. In large part, these changes can be seen as a business reaction by the platforms to changing community attitudes, changing privacy obligations (ie, in order to avoid large fines) and a desire to garner and maintain the trust of their customers. However, the incidental benefits for the platforms are greater control over the use of their tools and the data that arises out of such use.

While generally welcome from a privacy point of view, these recent developments have necessarily resulted in less personalised digital marketing, requiring significant additional advertising spend to achieve the prior levels of returns/success from marketing activities. One possible (and currently growing) means to combat this is for organisations/marketers to build a first-party (ie, direct organisation to customer) data relationship and ensure a privacy-first approach to overcome the impact of these changes, while meeting both privacy legal requirements and customer trust expectations. From a digital marketing point of view, failure to adapt will entrench the need for an ever-increasing marketing spend for ever diminishing returns.

What is a first-party data approach?

In order to be sustainable and effective, organisations/marketers must anchor their approach to personal information collection and use for marketing in a stronger one-to-one relationship with their customers and on a trust and exchange of value basis.

The first-party data approach does not rely on third-party collection of (or tools to collect) personal information and seeks to engage directly with each relevant customer. In addition, this approach also avoids the various concerns with third-party collections and assists with the increasingly difficulty issue of ensuring the trust of your customers in such circumstances. This approach includes focussing on four key areas:

- a data invitation
- having a data preference (or similar) centre
- having an ongoing data conversation
- communicating a value proposition or exchange

A "data invitation" appears trite but it is fundamentally a reimagining of the initial contact with/collection of the personal information of individuals and the notice that accompanies such. It departs from the current voluminous and often jargon-filled privacy notifications where individuals simply click and move on to viewing the content, making the purchase or engaging in the activity, with little idea of what they are actually "agreeing" to or "accepting". A data invitation requires precise and concise words and overtly clear language around the personal information being collected and what it will be used for. Some examples of this have included the use of pictograms or diagrams to simplify the message, significantly cutting down the wording of privacy notices and drafting the data invitation in "plain English". Furthermore, short explanatory videos have been used to demonstrate that the organisation is not just another faceless entity and to better explain the key aspects of the relationship (ie the information collected and the purposes it will be used for). This first-party data approach not only addresses the relevant notice (and any consent) requirements but will also assist to future proof the organisation against the upcoming announced changes to Australian privacy law in relation to marketing. It should also reduce the friction with customers (and the groups that represent them) by building a transparency-based trust.

A "data preference centre" provides transparent communication tools for existing privacy and security measures to build trust and gain customer buy-in. The key focus of the centre is to present the customer with a dashboard/tool that provides a granular list of personal information that is being/has been/will be collected as well as a short description of how (for what purposes) such will be used. However, this needs to include not only the specific personal information being directly collected from the customer but also any additional data that may be created or collected by using device identifiers, AI analytics or similar tools. For example, where geolocation data will be collected by reference to the device ID or profiling "assumptions" are created by using AI analytics, these should be explicitly noted along with the opportunity for the individual to "opt-out" of providing (or allowing the collection, creation and/or further use) of such information.

While this may initially result in less personal information being collected, the benefit to organisations is that customers will trust the organisation with and feel more in control of their personal information which, ultimately, will make them more inclined to share their personal information for marketing. Currently such preference centres are mostly associated with large tech providers, the platforms and a growing number of large Australian financial services organisations. In the latter case this has, anecdotally, significantly lessened customer complaints.

The aim of fostering a "data conversation" is to ensure that the "data relationship" is managed on an ongoing basis, so that organisations and their customers are engaging with each other about how the data is being used. In addition to increasing transparency, continued engagement serves as a reminder that the organisation is striving to improve its practices as regards personal information collection, use and security and, where such is the case, is utilising that customer's personal information to improve their overall experience with the product/service. While, admittedly, not all customers will want to invest the additional time in an ongoing data conversation, this approach will assist to future-proof organisations against both developing community attitudes and announced changes to the Australian privacy regime, once legislated. This continuing conversation can also help organisations justify keeping (if necessary) relevant marketing personal information beyond the period which would otherwise be allowed under Australian privacy law (ie under APP 11.2).

Finally, learning from the example of the loyalty programs employed across numerous sectors, putting a value exchange at the centre of the personal information collection relationship and clearly articulating the "value proposition or exchange" will help ensure that customers stay engaged with (and keep giving their personal information to) the organisation for marketing. To be clear, this is not to suggest a monetary payment for personal information. Rather, this approach is aimed at promoting a demonstrated value exchange for customers over the life of the relationship, which can take many forms including discounts, special privileges or improvements to the customer experience where relevant personal information is provided. These can all create a compelling value proposition including by helping customers better find what they are looking for more quickly, directing them to new products and services that are most likely relevant to them and, overall, improving the customer experience.

Organisations that can get this right will be better positioned to get the most out of their data (including personal information) and maintain their access to advise on it.

What is a privacy-first approach?

While self-explanatory and addressed, at least in part, in the discussion of the "first-party data approach" above, a "privacy-first" approach to marketing is to ensure that the privacy of the customer is considered as an essential part of (and built into) any digital marketing from the beginning. A "privacy-first" approach seeks to not simply comply with the relevant privacy regime but to exceed it by implementing industry better practice.

In the Australian context, this involves clear, overt and transparent language and processes to ensure visibility of the notification of what is being collected, the purposes for which it is collected and how a customer can "opt-out". This needs to be supported by the implementation of both rigorous internal limitations on the organisation's misuse (or additional use) of the relevant personal information together with a tool to give more granular control to the customer over the collection, use and disclosure of their personal information in relation to marketing. It also requires asking, at every key step, is this best (or at least acceptable) "privacy-wise" for the customer.

Australian privacy law does not yet require a privacy-first and first-party data approach to digital marketing. However, based on the announced changes to the Australian privacy law as regards marketing, they will become much more relevant (and possibly required) when the announced amendments are legislated during the course of 2024 and 2025.

For example, the announced changes to the Australian privacy and marketing regime will require more control to be provided to individuals whose personal information is used for marketing. Some of the changes include the introduction an unqualified right to opt-out of personal information being used for direct marketing and the creation of industry codes that specify what controls or rights consumers will have over their personal information as used in marketing. In addition, and while we are yet to see the exact wording of the proposed changes, it is clear that an ongoing data conversation will be essential for the sustainability and longevity of personalised digital marketing by organisations in the future.

Key takeaways/what you can do now

In order to get the most out of your current digital marketing and to future-proof it against the announced changes to privacy and marketing, organisations should:

- undertake an independent review of your marketing department's collection, use and disclosure of personal information, focussing on from where and how such information is obtained, as well as what limits/controls are imposed on such use to ensure personal information is only used in accordance with the notified purposes of collection
- uplift any of the identified compliance gaps and implement appropriate better practices to future-proof your marketing program
- ensure that the treatment of any personal information created or collected, other than directly from the individual, is clearly addressed in the notices (eg, geolocation data or new data created as a result of AI analytics/profiling)

- ensure that your marketing program deletes or de-identifies personal information in accordance with APP 11.2 (or implements a "data conversation" to allow for it to be kept longer)
- communicate the benefits of providing their relevant personal information for marketing, including as to any value proposition or exchange for the collection and use of their personal information for marketing
- consider extending additional rights to customers whose personal information is collected and used for marketing in the form of a preference centre where they can control when their personal information is collected and where and how it is used (ie, don't wait until the announced changes are legislated)
- investigate and determine what uplift is required and the steps necessary to implement a privacy-first and first-party data approach to your digital marketing to prepare you for compliance with the announced changes, once they are legislated

Alec Christie
Partner
Clyde & Co
Alec.Christie@clydeco.com
www.clydeco.com

Click "Accept All" to these new privacy reforms

***Andrea Beatty**, **Jennifer Fu** and **Jack Shaw** PIPER ALDERMAN*

Privacy Act Review

Privacy reforms are high on the Federal Government's agenda, including a public consultation addressing doxing and a comprehensive review of credit reporting provisions within the Privacy Act 1988 (Cth) in enabling effective lending decisions by credit providers whilst ensuring the adequate protection of consumers' personal information.[1]

Doxing is the "intentional online exposure of an individual's identity, private information or personal details without their consent".[2] Although doxing is often motivated by wanting to expose and hold a wrongdoer to account, it effectively violates the target's privacy and likely compromises their safety.[3] Despite its current multi-pronged approach, the Federal Government intends to enhance protections for individuals by introducing new provisions to the Privacy Act, including a new statutory tort and granting greater control and transparency to individuals over their personal information.[4]

On 16 February 2023, the Attorney-General's Department (Attorney-General) released the *Privacy Act Review* Report (Report).[5] The proposed reforms to Australian privacy laws aim to "[strengthen] the protection of personal information and the control individuals have over their information".[6] They include enhanced requirements in relation to the security of personal information and its destruction when no longer needed.

On 28 September 2023, the Federal Government published its response to the Report, titled *Government Response to the Privacy Act Review Report* (Response).[7] The Government agrees to 38 proposals, agrees in-principle to 68 proposals and notes 10 proposals.

Background

The increasing presence of digital services in the lives of Australian consumers reflects the significant benefits generated by digitisation, including consumer convenience and improved efficiencies.[8] It has also led to the collection, use, disclosure and storage of large amounts of personal information by businesses.

Privacy is highly prioritised by Australians, with 83% of individuals surveyed by the Office of the Australian Information Commissioner (OAIC) in 2023 indicating that they want more control and choice over the collection and use of their personal information.[9] Ironically, many consumers are unaware of the full extent of data accessible to businesses and the consequent growing power they hold over consumers.[10]

The Report notes that thousands of "data points" — unique identifiers representing an individual customer's actions, devices, location etc — are used to create a "360 view" of them.[11] This triggers a concern for abusive data practices which businesses may engage in when marketing to individuals, which will be the primary focus of this article, and the increased occurrence of serious data breaches.[12]

Presently, the Australian privacy framework enables businesses to accumulate data without stringent restrictions or transparency requirements.[13] For example, information relating to customers may be used to target consumers with personalised marketing content without the need to identify who they are. This places such information outside the definition of "personal information", and the full operation of the Privacy Act.[14] Concerningly, the framework provides scarce protections for children from predatory marketing practices online. It is estimated that 72 million data points are collected on a child before the age of 13. This statistic illustrates the troubling potential for the manipulation and restriction of a child's decisional autonomy, due to their vulnerability and lack of cognitive judgement.[15]

In response to a series of high-profile data breaches in 2022, the Federal Government introduced heightened enforcement powers for privacy regulators and substantially increased the maximum penalties for contravening the Privacy Act. However, these implementations are unlikely to change companies' marketing practices unless the substantive rules underpinning data collection and use undergo reform.[16]

Objectives of the privacy reforms

The Australian privacy laws have notably lagged behind advancements in the digital economy, where legislative loopholes are potentially exploited by businesses whose marketing practices use data to "track and target" consumers of all ages.[17] Consequently, sweeping reforms were put forward to modernise a framework that was no longer considered "fit-for-purpose" in the current digital age.

In recognition of such legislative shortcomings, the proposed reforms will:

- enable individuals to exercise new privacy rights
- establish stronger privacy protections for children and
- enhance requirements relating to the security of personal information and its destruction when no longer needed[18]

The Response categorises the Report's proposals under five focus areas, as outlined below:

- Bring the Privacy Act into the digital age — a framework that balances the public interest in protecting an individual's privacy and digital innovation. This involves removing existing exemptions relating to small businesses, employee records, political entities, and journalism to broaden the scope and application of the Act.[19]
- Uplift protections — a framework that recognises that self-management inadequately ensures individual privacy, and leaves consumers vulnerable to devastating data breaches. By imposing further obligations, additional guidance, and heightened accountability standards for entities, the reforms aim to foster a proactive approach to privacy risk management that better accounts for society's most vulnerable.[20]
- Increase clarity and simplicity for entities and individuals — a framework that promotes innovation and confidence amongst entities by clarifying and simplifying the Act's operation.[21]
- Improve control and transparency for individuals over their personal information — a framework that grants individuals greater transparency and control over their personal information through the introduction of enhanced consent and notice mechanisms, and the creation of new individual rights.[22]
- Strengthen enforcement — expanding the OAIC's enforcement powers and the scope of orders a court can make in civil penalty proceedings.[23]

Overview of proposed reforms relating to marketing

The Report proposes nine reforms to Australia's privacy framework which specifically focus on marketing.[24] With the exception of Proposal 20.3 which has been "noted" by the Federal Government, the remaining 8 proposals had been "agree[ed to] in-principle". This indicates that the Attorney-General will conduct further engagement with entities and a comprehensive impact analysis, which in turn informs any further consideration of a proposal's implementation by the Government.[25]

Set out below is an overview of the key aspects of the proposed reforms relating to marketing:

- Definitions
  - — targeting — defined as the collection, use or disclosure of information relating to an individual, which includes personal information, deidentified information and unidentified information, for purposes beyond marketing[26]
  - — trading — disclosing personal information for a benefit, service, or advantage[27]
  - — direct marketing — extends beyond promoting goods or services, to include promoting any organisation's aims and ideals[28]
- Greater choice and control
  The framework intends to introduce new rights for individuals and impose a new obligation on entities to strengthen the control which individuals have over their personal information. These proposed changes are as follows:
  - — Unqualified right to opt-out of use or disclosure of personal information for direct marketing — to regulate unsolicited marketing contact, which would apply generally to more traditional forms of direct marketing as well as circumstances where targeting reaches the threshold of direct marketing. On exercising this right, an entity must not use or disclose personal information for direct marketing.[29]
  - — Unqualified right to opt-out of receiving targeted advertising — provides individuals with the benefit of stopping targeted advertising from being presented to them. By also suggesting that consent be required for targeting, individuals effectively gain greater control over their personal information.[30]
  - — Requirement of consent to trade in personal information — ensures that individuals are informed and that they agree to disclosing their personal information to a third party. Individuals have the right to withdraw their consent at any time.[31]
- Prohibitions on harmful practices
  The Report intends to introduce the following prohibited practices to the privacy framework:
  - — Direct marketing to children — personal information must be collected directly from the child, where direct marketing is in the child's best interests.[32] Currently, parental or guardian consent is not required to be provided on behalf of a child who is under the age of 16.[33] Although this issue was raised in the Attorney-General's Discussion Paper on the *Privacy Act*

Review (Discussion Paper),[34] there was no proposed amendment requiring parental or guardian consent where the child is under the age of 16 in connection with direct marketing to a child.[35]

— Targeting children — prohibited except where targeting is in the child's best interests. A blanket prohibition may interfere with the development of beneficial services that entail minimal privacy risks.[36]

— Trading in children's personal information — supporting the prohibition against targeting children. Over 50% of apps reviewed in an Audit of Android entertainment apps demonstrated "some level of problematic data collection behaviour".[37]

— Targeting which exploits vulnerability, manipulates, discriminates and excludes — ensuring individuals are confident that targeting is conducted safely and ethically. Submitters support prohibiting the handling of information such that it causes harm or discriminates, as well as targeting directed at vulnerable individuals.[38]

— Targeting based on sensitive information and traits — maintaining consistency with current industry practices.[39]

- Fair and reasonable test
  This test requires entities to ensure that entities collect, use or disclose information relating to an individual in a fair and reasonable manner, depending on the circumstances. Not only does this allow for flexibility when addressing targeting that aims to manipulate, exploit or undermine autonomy, the test would also encourage greater fairness and transparency.[40]
- Greater transparency
  To promote greater awareness and understanding amongst consumers on the operation and reasons for targeting, the framework proposes that entities should provide such information to online users and make it publicly available.[41]

Concluding notes and next steps

The Report and Response have shown that the Federal Government views the overhaul of Australia's privacy framework as a long-term project. The series of proposals constitutes some of the most extensive reforms proposed for the Privacy Act since its inception. While certain reforms align certain aspects of Australia's privacy regulations with global counterparts like the General Data Protection Regulation, they also ensure the preservation of Australia's distinctive privacy framework. The Federal Government has indicated that it intends to introduce legislative amendments in 2024, an anticipated first step in a sequence of reforms. In the meantime, the Attorney-General will be involved in developing "agreed" proposals in line with detailed impact analyses and will engage in targeted stakeholder consultations regarding the feasibility of proposals which the Government "agreed in-principle" on.[42]

Andrea Beatty
Partner
Piper Alderman
abeatty@piperalderman.com.au
https://piperalderman.com.au/

Jennifer Fu
Law Graduate
Piper Alderman
https://piperalderman.com.au/

Jack Shaw
Law Clerk
Piper Alderman
jwshaw@piperalderman.com.au
https://piperalderman.com.au/

Footnotes

1. Privacy Act 1988 (Cth).
2. Attorney-General's Department, Public Consultation on Doxxing and Privacy Reforms, March 2024, accessed 3 April 2024 https://consultations.ag.gov.au/integrity/doxxing-and-privacy-reforms/.
3. eSafety Commissioner, Doxing, March 2024, accessed 3 April 2024, www.esafety.gov.au/industry/tech-trends-and-challenges/doxing.
4. Above n 2.
5. Attorney-General's Department *Privacy Act Review* Report 2022 (2023) www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf.
6. Above.
7. Attorney-General's Department *Government Response to the Privacy Act Review* Report (2023) www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF.
8. Above n 5.
9. Attorney-General's Department *Government Response to the Privacy Act Review Report* Fact Sheet (2023) www.ag.gov.au/sites/default/files/2023-09/fact-sheet-government-response-privacy-act-review-report.PDF.

10. K Kemp "Australia's privacy laws demand reform to better protect consumer" *UNSW Law & Justice* 7 June 2023 www.unsw.edu.au/law-justice/our-research/impact/australia-privacy-laws-demand-reform-better-protect-consumers.
11. Above n 5, at 198.
12. Above n 10.
13. Above.
14. Above n 5, at 3.
15. Above n 5, at 216.
16. Above n 10.
17. Above n 10; above n 5, at 146.
18. Office of the Australian Information Commissioner "OAIC welcomes reforms critical to Australia's privacy future" media release (28 September 2023) www.oaic.gov.au/newsroom/oaic-welcomes-reforms-critical-to-australias-privacy-future.
19. Above n 7, at 5–7.
20. Above n 7, at 8–14.
21. Above n 7, at 3.
22. Above n 7, at 17–18.
23. Above n 7, at 20.
24. Above n 5, at 12–13.
25. Above n 5, at 2.
26. Above n 5, at 210.
27. Above n 5, at 211.
28. Above n 5, at 210.
29. Above n 5, at 211.
30. Above n 5, at 212–13.
31. Above n 5, at 214.
32. Above n 5, at 215.
33. Above n 5, at 147.
34. Attorney-General's Department *Privacy Act Review* Discussion Paper (2021) https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf.
35. Above, at 12–13.
36. Above n 5, at 216.
37. Above n 5, at 217.
38. Above.
39. Above n 5, at 218.
40. Above.
41. Above n 5, at 219–20.
42. Above n 7, at 4.

For editorial enquiries and unsolicited article proposals please contact Monica Nakhla at monica.nakhla@lexisnexis.com.au
Cite this issue as (2024) 21(1) *PRIVLB*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN 1449-8227 Print Post Approved PP 243459/00067