*University of New South Wales Law Research Series*

# SUBMISSION IN RESPONSE TO THE AUSTRALIAN COMPETITION & CONSUMER COMMISSION AD TECH INQUIRY PAPER

**KATHARINE KEMP**

[2020] *UNSWLRS* 26

UNSW Law
UNSW Sydney NSW 2052 Australia

**E:** unswlrs@unsw.edu.au
**W:** http://www.law.unsw.edu.au/research/faculty-publications
**AustLII:** http://www.austlii.edu.au/au/journals/UNSWLRS/
**SSRN:** http://www.ssrn.com/link/UNSW-LEG.html

# Submission in Response to the Australian Competition & Consumer Commission Ad Tech Inquiry Issues Paper

Dr Katharine Kemp, Academic Lead, UNSW Grand Challenge on Trust
Senior Lecturer, Faculty of Law, UNSW Sydney

26 April 2020

This submission is made by Dr Katharine Kemp, Academic Lead, UNSW Grand Challenge on Trust, and Senior Lecturer, Faculty of Law, in response to the Ad Tech Inquiry Issues Paper (Issues Paper) of the Australian Competition and Consumer Commission (ACCC), as part of the UNSW Grand Challenge on Trust.

UNSW's Grand Challenge on Trust aims to deepen our understanding of trust, of distrust, and their effects on society. In a time when we are asked to trust institutions, companies, technology and experts, and give our personal data more freely, it has never been more crucial to interrogate the concept of trust. By building interdisciplinary networks, and facilitating critical discussions, the Grand Challenge examines the nature of trust deficits, abuses of trust, the consequences of declining or improved trust, and what is necessary to become worthy of trust.

The views in this submission are my own, based on my research, and do not represent the official views of UNSW Sydney.

This submission does not attempt to address all topics raised by the Issues Paper, but is limited to the following:

- Some aspects of competition throughout the ad tech supply chain; and
- The role and use of data in supplying ad tech services.

**Summary:**

Both the ACCC Digital Platforms Inquiry (DPI) Final Report and the Ad Tech Inquiry Issues Paper identify that there is a lack of transparency in ad tech markets, particularly in respect of the proportion of advertising spend retained by ad tech vendors and verification that the promised services have actually been delivered. Price signals are obscured and marketers have limited ability to negotiate for better, verified outcomes, especially in their dealings with Google and Facebook as the central channels for online advertising. But an ad tech inquiry which focuses on these issues alone would be incomplete.

An examination of the data practices of the ad tech sector will be vital to a comprehensive understanding of competition in these markets and its impact on consumers. The ad tech sector is founded on consumers' personal data. Consumer profiling and segmenting, behavioural advertising, measurement and attribution are sustained by ever-increasing collection and use of personal data. Indeed, ad tech vendors market their services on the quantities of this data to which they have access; the millions of insights on individual consumers.

At the same time, publishers, marketers and ad tech vendors are aware that many consumers would be uncomfortable with the knowledge that their behaviour is pervasively monitored and tracked for commercial gain. Privacy policies are therefore replete with "marketing speak" intended to persuade consumers to accede, as well as opaque and open-ended terms intended to give companies maximum permission to use consumer data for their own ends. Ad tech players constantly invest in new ways to circumvent consumers' attempts to avoid the monitoring of their daily behaviour. There are also spurious claims that many practices use only "de-identified", "anonymised" or "non-personal" information, while producing a detailed profile of the individual consumer.

While many ad tech businesses have profited from these strategies, lack of transparency about data practices and the cost and effectiveness of targeted or behavioural advertising hinders publishers' and marketers' ability to determine whether these methods are, on balance, the most efficient way of serving their own interests or whether less intrusive methods would better serve them and their customers.

The degradation of consumer data privacy causes objective detriment to consumers and undermines the competitive process. As I have explained more thoroughly in an earlier paper, concealed data practices make consumers more susceptible to criminal activity, discrimination, exclusion, manipulation and humiliation, and undermine consumer trust in beneficial digital initiatives.[1] This is not only problematic in terms of consumer protection and privacy regulation. These data practices chill competition on privacy quality; preserve substantial market power by means other than superior efficiency; and deepen information asymmetries and imbalances in bargaining power.

Those anticompetitive effects are felt directly in markets for the products consumers acquire themselves. In this submission, I argue that the externalities and distortions from degraded privacy protection also compromise the efficiency of advertising markets. Even if the services supplied in ad tech markets were perfectly transparent to marketers and publishers and the algorithms and auctions were perfectly calibrated to allocate between clients, they are based on a fundamental distortion resulting from concealed data practices.

Supporting, implementing and enforcing the reforms to Australian privacy law recommended by the ACCC in the Digital Platforms Inquiry (DPI) Final Report will be an essential first step in removing these obstacles

[1] Katharine Kemp, 'Concealed Data Practices and Competition Law: Why Privacy Matters' (UNSW Law Research Paper No 19-53, 6 August 2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3432769.

to competition on privacy quality and preventing ad tech vendors from continuing to externalise the cost of privacy-degrading data practices.

## 1. Data privacy as an aspect of competition in the ad tech supply chain

In considering the degree of competition in various markets in the ad tech supply chain, it is necessary not only to consider the prices paid for ad tech services, but the quality of those services, including their impact on the data privacy of publishers' audiences and marketers' customers.

### 1.1 Actors in ad tech markets

Each display advertising transaction involves:

- a **publisher** who sells advertising opportunities ("ad inventory") and publishes the advertisement to its audience, for example, on its website, app, podcast, or programmatic television;
- a **marketer** who purchases the opportunity to market its product to the consumer by displaying an advertisement on that site, and thus seeks to gain, retain, or increase its profit from, customers; and
- the **consumer** who visits the site where the advertisement is displayed, and whose behaviour is often tracked before and after this display. The consumer is both a member of the publishers' audience and an actual or potential customer of the marketer.

This advertising transaction is frequently conducted with the assistance of a number of **third-party ad tech vendors** who aim to facilitate the purchase and/or sale of ad inventory; finer targeting of consumers; and the measurement and attribution of the consumer's behaviour following the advertisement. In so doing, each vendor takes a cut of advertising expenditure and frequently collects and discloses consumers' personal data.

These vendors are third parties in the sense that they are neither the publisher selling the ad inventory nor the marketer purchasing the advertising opportunity. These include supply side platforms; ad exchanges; demand side platforms; and ad verification, attribution and measurement providers. Data brokers; data analysts; and data management platforms also provide data services which contribute to these transactions.

Although the average consumer is unlikely to recognise the name of any of these entities as ad tech vendors, their personal data may be handled by thousands of them.[2] Ad tech businesses often compete to provide publishers and marketers with services on the basis of the number of consumers they profile (generally numbering in the millions); the accuracy with which they can identify individual consumers; and the level of detail and real-time information their consumer profiles contain.

### 1.2 Who is the consumer?

In this submission, where the word "consumers" is used without qualification, it refers to publishers' audience members and/or marketers' actual and potential customers.

[2] See Information Commissioner's Office, United Kingdom, 'Update Report into Adtech and Real Time Bidding' (Report, 20 June 2019) 20, on the number of organisations involved in a single transaction. See further Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 14, referring to the "thousands of interconnected entities" that generally "do not have any direct relationship with users".

Suppliers of ad tech services sometimes imply in their marketing and other documentation that they in fact supply advertising services to individual consumers.

For example, the Google Privacy Policy states that:

> *We use automated systems that analyse your content to provide you with things like customised search results, personalised ads or other features tailored to how you use our services.*

Commentators and stakeholders also argue that targeted advertising creates benefits for consumers, particularly in the form of reduced search costs, seeing advertisements which are more relevant to them and supporting zero-priced online content.[3]

However, it would be difficult to argue that individual users of internet search, social media or online news are consumers of digital display advertising, given that they are generally subjected to this advertising rather than exercising any direct choice in its selection or display.[4] Still less are they consumers of other ad tech services, bearing in mind that they are generally unaware of the existence of these services.

The consumers of ad tech services are not individuals, but firms in the role of publisher or marketer for the purpose of the advertising transaction. Where publishers and marketers are referred to in this sense, this submission will use the term "clients".

### 1.3 Consumer privacy as an aspect of ad tech service quality

The utility of ad tech services for publishers and marketers does not only depend on returns on investment in their ad inventory and ad campaigns respectively. It also depends on the impact of the ad tech services on consumers.

For example, if publishers' audiences are shown low quality advertisements or advertisements which tarnish the publishers' image, this reflects lower quality in ad tech services. This would also be the case if a marketer's customers were spammed or subjected to excessive retargeting following interaction with the marketer's advertisement.

**The effect of ad tech businesses' data practices on consumer privacy should be taken into account as an aspect of the quality of ad tech services and as a reflection of the degree of competition in the market.**

If, for example, publishers wish to provide their audiences with a privacy-respecting website but are unable to negotiate with a major supplier of ad tech services for better consumer privacy terms, this should be taken into account in determining whether that supplier possesses substantial market power.

General trends in the effects of ad tech data practices on consumer data privacy are discussed in the second part of this submission.

The Commission should consider the effect of these data practices to determine:

- their impact on consumer welfare[5] per se;

[3] See, eg, David S Evans, 'The Online Advertising Industry: Economics, Evolution, and Privacy' (2009) 23 *Journal of Economic Perspectives* 37, 57; David S Evans, 'Mobile Advertising: Economics, Evolution and Policy (2016) 30-34, 47.

[4] Cf David S Evans, 'The Online Advertising Industry: Economics, Evolution, and Privacy' (2009) 23 *Journal of Economic Perspectives* 37, 41, has argued that "consumers are 'paid' with content and services to receive advertising messages'.

[5] "Consumer welfare" is used here in the broad sense rather than the strict competition law sense.

- their effect on competition in relevant markets, particularly where the practices hinder competition from privacy-enhancing alternatives;
- whether there are potential infringements of the Australian Consumer Law that should be investigated by the Commission;
- whether there are potential infringements of the *Privacy Act 1988* (Cth) that should be referred to the Office of the Australian Information Commissioner; and
- whether there is evidence that will be relevant to recommendations for reform in the forthcoming review of the *Privacy Act*.

### 1.4 The debatable advantages of behavioural advertising

Numerous ad tech services are designed to support a particular type of advertising, namely behavioural advertising. Behavioural advertising purports to use data about consumers' past behaviour to match the relevant advertisement to an individual who is likely to respond to that advertisement. As such, it is promoted as highly efficient on the basis that it reduces wasted advertising expenditure and consumer search costs.[6] However, as discussed later in this section, a number of stakeholders have expressed growing misgivings about the superiority of behavioural advertising.

Behavioural advertising can be contrasted with more traditional **broadcast advertising**. Broadcast advertising displays the same advertisements to all members of a wider audience – everyone watching a certain television channel or listening to a particular radio station – even though a large percentage of that audience will have little interest in the product in question and little prospect of buying it in the near future. For example, all viewers of the six o'clock news will be shown the same advertisement for discount power tools. Broadcast advertising may result in a substantial proportion of wasted advertising expenditure due to the large number of mismatched consumers: those viewers of the six o'clock news who have no interest in power tools, for example.

Behavioural advertising can also be distinguished from **contextual advertising**, which changes the advertisement displayed based on the immediate context of the app or website interaction.[7] In the digital context, for example, when a person enters "meal replacement shakes" in a search engine, the search results page may display contextual advertisements for protein shakes, weight loss programs and fitness accessories. When a person browses a trail running blog, the blog webpage may display contextual advertisements for trail running shoes and camping holidays. Contextual advertising improves efficiency by selecting the advertisement to be displayed based on inferences that can be made about the consumer's interests from the short-term interaction.[8]

**Behavioural advertising**, on the other hand, selects the advertisement displayed based on the profile of the individual who is believed to be watching that advertisement, or a segment of consumers to which that individual has been allocated. That profile or segmentation is in turn based on the assumed interests and characteristics of the person in question, which are inferred from that person's behaviour online (and

[6] See Katherine J Strandburg, 'Free Fall: The Online Market's Consumer Preference Disconnect' (2013) *University of Chicago Legal Forum* 95, 102-105. Cf Omid Rafieian and Hema Yoganarasimhan, 'Targeting and Privacy in Mobile Advertising' (Working Paper, 30 January 2020), arguing that contextual advertising may be more effective than behavioural advertising.

[7] Katherine J Strandburg, 'Free Fall: The Online Market's Consumer Preference Disconnect' (2013) *University of Chicago Legal Forum* 95, 99.

[8] See Omid Rafieian and Hema Yoganarasimhan, 'Targeting and Privacy in Mobile Advertising' (Working Paper, 30 January 2020), arguing that contextual advertising may be more effective than behavioural.

sometimes offline) over time.[9] For example, if a person has been browsing the "for sale" section of an online real estate platform and using the interest rate calculator on their bank's website, the person may be shown advertisements for home loans while browsing the weather website.

Behavioural advertising can also be significantly more subtle and manipulative.[10] For example, an online profile developed about a consumer could reveal that the consumer is female, between 17 and 19 years old, has read online articles about how to use make-up to diminish nose size, and interacts with social media in a way that reveals she tends to feel most depressed and unattractive on Monday mornings.[11] This information could be used to target young women with a similar profile with advertisements for cosmetic procedures at the start of the week. Alternatively, consumers who have searched for "chronic pain management" in a search engine may be shown pharmaceutical advertisements for dangerous opioids with escalating messages on various other websites they visit.[12]

Behavioural advertising relies on far greater collection, use and storage of personal data than contextual or traditional advertising, since it depends on profiling and targeting consumers based on data about their past behaviour and not merely their immediate interaction with the publisher.[13]

Notwithstanding the claims made regarding the efficiency of behavioural advertising, strong doubts have been raised about its superiority relative to contextual advertising in particular. Research suggests that, for publishers, there may be very little increase in revenue from behavioural, as opposed to contextual advertising.[14] Publishers also complain of the degradation of high-quality online content when audience targeting, rather than content quality, becomes the focus.[15]

Marketers have complained of a general lack of transparency in the ad tech supply chain; unacceptable levels of ad fraud; and the wastefulness of the "ad tech tax" claimed by the numerous third-party vendors in the programmatic, behavioural advertising supply chain.[16]

---

[9] See Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 102.

[10] See, eg, Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy and Manipulation' (2019) 8 *Internet Policy Review* (forthcoming); Ryan Calo, "Digital Market Manipulation" (2014) 82 *George Washington Law Review* 995; Ryan Calo and Alex Rosenblat.

[11] See Lucia Moses, 'Data Points: Talk to Her' (Adweek, September 2013) 16, identifying that "[w]omen feel ugliest on Mondays and weekends', as well as 'The Top 5 occasions when women feel least attractive'.

[12] See Alison Branley, 'Google Search Data Used by Pharma Giant to Bombard Users with Ads for Addictive Opioids' (ABC Online, 13 July 2019).

[13] See George J Stigler Center for the Study of the Economy and the State and The University of Chicago Booth School of Business, 'Stigler Committee on Digital Platforms: Final Report' (September 2019) 44-45.

[14] See, eg, Veronica Marotta, Vibhanshu Abhishek and Alessandro Acquisti, 'Online Tracking and Publishers' Revenues: An Empirical Analysis' (Preliminary Draft, May 2019).

[15] Joseph Turow, *The Daily You: How the New Advertising is Defining Your Identity and Your Worth* (Yale University Press, 2011) 84-86; George J Stigler Center for the Study of the Economy and the State and The University of Chicago Booth School of Business, 'Stigler Committee on Digital Platforms: Final Report' (September 2019) 63.

[16] Joseph Turow, *The Daily You: How the New Advertising is Defining Your Identity and Your Worth* (Yale University Press, 2011) 84; George J Stigler Center for the Study of the Economy and the State and The University of Chicago Booth School of Business, 'Stigler Committee on Digital Platforms: Final Report' (September 2019) 61-63; Ivan Guzenko, 'How Programmatic Evolved Within 8 Years' (Martech Advisor online, 7 November 2019): "Programmatic chains may disclose little to no information regarding what part of the impression cost reaches the publisher after service commissions and margins are subtracted from the total sum."

Behavioural advertising has also given rise to an ever-increasing number of firms relying on vague, opaque terms in lengthy privacy policies to broadly use and disclose personal data for commercial gain, without the knowledge of consumers.[17]

Lack of transparency about the cost of, value added by, and data flows required by ad tech services in the supply of behavioural advertising hinders the introduction of privacy preserving subscription models for online content, as well as privacy preserving methods of targeted advertising, such as those based on data which does not leave the consumer's browser.[18] This lack of transparency also makes the question of whether contextual advertising has comparable or superior welfare effects more difficult to answer.

It seems increasingly likely that consumer data privacy is being sacrificed in the data "free-for-all" of online behavioural advertising in the absence of evidence of a proportionate increase in the quality and efficiency of advertising for publishers, marketers or consumers.

## 2. The role and use of data in supplying ad tech services

### 2.1 Consumer attitudes and "big data" imperatives

Consumers are increasingly concerned about their online privacy.[19] Surveys reveal that consumers often feel they lack real information or choices about how their personal data is collected or used. The majority believe that they should be given options about whether their data is used for purposes other than the original purpose for which it was provided.[20]

The ACCC's earlier research has revealed that most Australian users of digital platforms consider certain tracking, targeting and profiling data practices to be misuses of their personal data. These include, when the consumer is not logged in to a service:

- keeping track of the consumer's online behaviour such as the consumer's browsing history, viewing habits or search history;
- creating profiles or enabling targeted advertising; or
- using the information the platform has on the consumer (including from third parties) to show the consumer personalised advertisements.[21]

In light of these consumer attitudes, it is especially concerning that these data practices are in fact commonplace, particularly in the context of ad tech services and other data-funded businesses.

An individual consumer's personal data is daily passed between hundreds, sometimes thousands, of firms most consumers have never heard of. This personal data is used for commercial purposes well beyond the purpose for which the consumer originally provided their information. Further, a large proportion of data is

[17] Explained in section 2.6 below.

[18] See, eg, Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum and Solon Barocas, 'Adnostic: Privacy Preserving Targeted Advertising' (Network and Distributed System Symposium, March 2010).

[19] Office of the Australian Information Commissioner, 'Australian Community Attitudes to Privacy Survey 2017' (2017) 17.

[20] Phuong Nguyen and Lauren Solomon, 'Consumer Data and the Digital Economy: Emerging Issues in Data Collection, Use & Sharing' (Consumer Policy Research Centre, 2017) 4, 36-38.

[21] ACCC, 'Digital Platforms Inquiry: Final Report' (June 2019) 389-390. Similarly, the Office of the Australian Information Commissioner, 'Australian Community Attitudes to Privacy Survey' (2017) ii revealed that:

- only 21 percent of Australians were comfortable with targeted advertising based on their online activities; and
- only 17 percent of Australians were comfortable with social networking companies keeping databases of information on their online activity.

collected without any action or awareness on the part of the consumer, using digital surveillance tools which track individual behaviour online and offline. This profusion of tracking, collection and disclosure is almost entirely invisible to the average consumer.

These data practices are driven by three commercial imperatives in particular. First, firms have increasingly sought to accumulate vast amounts of "big data", including personal data, for the purposes of applying machine learning to extract new commercial insights from that data.[22] Second, many firms seek to create highly detailed, individual consumer profiles for their own marketing purposes, or to sell to or exchange with other firms engaged in digital advertising.[23] Third, these consumer profiles and other personal data are used for the purposes of behavioural advertising, as well as measuring the performance of such advertising by tracking the consumer's subsequent behaviour.[24]

The competition to gain ever deeper "insights" and advantages from monitoring, profiling, segmenting and targeting consumers has driven firms to conduct such pervasive collection of personal data that it has been justifiably described as "surveillance".[25]

### 2.2 Programmatic advertising and real-time bidding

A large proportion of digital advertising takes the form of **programmatic advertising**. The advertising is programmatic in the sense that it is automated: a significant part of the advertising transaction is performed by algorithms, rather than directly negotiated by humans.

Some programmatic advertising takes the form of a direct deal negotiated between the publisher and marketer for a certain period of time. In other cases, programmatic advertising purchased by "real-time bidding", an algorithmic auction involving a number of third-party ad tech vendors.[26]

The essence of the **real-time bidding process ("RTB")** is as follows.[27] When a consumer uses an app or browses a website, the publisher has an opportunity to sell certain advertising space. While the web page or app is loading, an automated auction takes place to determine which marketer will have the right to place an advertisement in each of the available advertising spaces and at what price. A similar process may take place when a consumer listens to a podcast or views a program on a connected television.

---

[22] See, eg, Viktor Mayer-Schönberger and Thomas Ramge, *Reinventing Capitalism in the Age of Big Data* (John Murray, 2018) 77-78, 84-85.

[23] See Nico Neumann et al, 'How Effective is Third-Party Consumer Profiling and Audience Delivery? Evidence from Field Studies' (Working Paper, Forthcoming in Marketing Science-Frontiers, 12 June 2019) 2.

CoreLogic enjoins businesses to "[m]ake sure you are collecting all the data you can about your customers and their behaviours, make sure you can store and link it to internal and external data to create insights, and most important know how you can use those insights to get better at service and at pro-actively meeting your customers' needs. If you aren't, someone else will." https://www.corelogic.com.au/resources/are-you-data-smart

[24] See section 1.4 above.

[25] See, eg, John Gilliom and Torin Monahan, *SuperVision: An Introduction to the Surveillance Society* (University of Chicago Press, 2013) 47 ff; Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 11; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile, 2019).

[26] See Interactive Advertising Bureau (IAB), *Programmatic 101 for Direct Sellers* (2014), defining 'programmatic' advertising as 'the process of executing media buys in an automated fashion through digital platforms such as exchanges, trading desks and demand-side platforms'. Aside from the sale of ad inventory via auctions, programmatic advertising can also take the form of "automatic guaranteed" and "preferred deals", both of which are automated and receive priority over purchases of ad inventory via auction.

[27] See further Information Commissioner's Office, United Kingdom, 'Update Report into Adtech and Real Time Bidding' (Report, 20 June 2019) 5, 8.

The publisher broadcasts a bid request and ultimately selects a winning bid from the numerous marketers who respond to the bid request. In the process, the publisher sends data about the consumer to various marketers and third-party ad tech vendors, allowing these firms to match the consumer visiting the website or app with other existing data on the consumer for the purposes of matching an advertisement to that visit.[28]

For example, some marketers may only be willing to bid for advertising inventory where the consumer is male, aged between 18 and 25, with an interest in Mardi Gras events; or a female, aged over 50, with an interest in incontinence products.

### 2.3 Disclosure of consumers' personal data in the ad tech supply chain

Throughout the ad tech supply chain, personal data is collected by and disclosed to numerous firms. These firms use the personal data to facilitate the ad placement but often retain that personal data for other purposes, including the creation of more detailed consumer profiles, feeding into the goals of big data accumulation and consumer profiling.[29]

It is not possible to categorise ad tech vendors according to the services they provide since a single firm may perform more than one of these functions in various combinations. This section therefore describes various key functions performed by ad tech vendors, and the types of data collected and disclosed, rather than suggesting fixed categories of service providers.

The special case of major platforms, which integrate a number of these functions internally, is explained further in the section 2.4 below.

**Supply side platforms** (SSPs) act on behalf of publishers to manage their ad inventory and optimize the price received for that inventory.[30] SSPs make the advertising opportunities on the publisher's app or website known to potential marketers by aggregating the advertising opportunities of various publishers.

When an ad is about to be loaded on an app or website, the SSP may facilitate the broadcast of a bid request on behalf of the publisher. The bid request can incorporate data about the person and/or device loading the app or website, which may include the URL of the website, device information (including brand, model and operating system), the consumer's location, the consumer's IP address, profile data compiled by data brokers, app usage, and/or other unique identifiers or profile information that allow marketers to determine whether they wish to bid for that ad placement.[31]

The personal data transmitted by the SSP as part of the bid request can be very revealing.[32] For example, the Norwegian Consumer Council has pointed out that a person's use of the Grindr app "is in itself a strong

[28] This matching is often performed without reference to the consumer's name, but through the use of other identifiers including device identifiers; advertising identifiers; encrypted email addresses; and other unique identifiers, as explained in section 2.5.2 below.

[29] Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 39.

[30] SSP services are, eg, provided by MoPub, Google Ad Manager, OpenX, AppNexus, Rubicon Project and PubMatic.

[31] See Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 36-37, 55-59; Information Commissioner's Office, United Kingdom, 'Update Report into Adtech and Real Time Bidding' (Report, 20 June 2019) 12-13. According to the ICO, this further information can include the consumer's online activity (scrolling, clicking, highlights, media views), search queries, session time and demographic data: at 13.

[32] Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 36, 55-59.

indicator of sexual preferences, as the app is geared toward homosexual, bisexual, and trans people".[33] The UK ICO noted that information included in the bid request may include categories such as 'Heart and Cardiovascular Diseases', 'Mental Health', 'Sexual Health', 'Infectious Diseases', 'Reproductive Health', 'Substance Abuse', 'Health Conditions', 'Politics' and 'Ethnic & Identity Groups'.[34]

The bid request is generally broadcast to various demand side platforms and other ad tech players.[35]

**Demand side platforms** (DSPs) act on behalf of marketers to assist with advertising campaigns, receive bid requests and allow marketers to bid in real-time for ad placements on publisher apps or websites.[36]

On receiving the bid request, DSPs and other third-party vendors wish to determine which marketers will be most interested in the relevant consumer for behavioural advertising purposes. To do this, they may seek to identify the consumer more closely by a process of "ID syncing" or "ID mapping". Essentially, various third-party vendors may already have data associated with the relevant consumer which they have received via their own third-party cookies[37] placed on the consumer's device. ID syncing or mapping synchronises the various pseudonymous identifiers the third-party vendors respectively associate with that particular consumer via their own cookies, allowing the vendors to identify the relevant consumer in their own databases.

The data contained in the bid request is used by the DSPs to determine whether a particular marketer should place a bid, but it may also be retained by third-party vendors to add to existing consumer profiles.

**Ad networks** also facilitate the sale of publishers' ad inventory. They collect digital ad inventory from numerous publishers, add a margin and sell packages of this ad inventory to marketers.

Ad networks may hold detailed profiles on large numbers of consumers which allow the networks to promise marketers the ability to target consumers who have specific characteristics via particular publishers.[38]

---

[33] Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 123.

[34] Information Commissioner's Office, United Kingdom, 'Update Report into Adtech and Real Time Bidding' (Report, 20 June 2019) 13.

[35] Ivan Guzenko, 'How Programmatic Evolved Within 8 Years' (Martech Advisor online, 7 November 2019): "Publishers collected the cookies of website visitors and offered them along with placement details, to advertisers (via SSP). If user data matched targeting details on DSP, AI and ML-based algorithms assessed the value of each impression, took part in the auction, and automatically closed the deals on behalf of advertisers."

[36] DSP services are, eg, provided by DataXu, Rocket Fuel, Adcash, AppNexus, SmartyAds, DoubleClick Bid Manager, Simpli.fi, The Trade Desk, MediaMath, and Amazon DSP.

[37] Cookies are small text files placed on a consumer's device which allow the originator of the cookie to retrieve information about the consumer which is stored in that text file over time. A third-party cookie is a cookie that originates from a party other than the operator of the website which the consumer is visiting. These are also referred to as "tracking" or "targeting" cookies. See further section 2.5.4 below on the "death" of the third-party cookie.

[38] See David S Evans, 'The Online Advertising Industry: Economics, Evolution, and Privacy' (2009) 23 *Journal of Economic Perspectives* 37, 41. See Joseph Turow, *The Daily You: How the New Advertising is Defining Your Identity and Your Worth* (Yale University Press, 2011) 74-78.

An **ad exchange** may sit between publishers and marketers, or between SSPs or ad networks and DSPs (although a number of SSPs now incorporate an ad exchange in their own services).[39] The ad exchange provides a central platform or market for the automated buying and selling of ad placements.[40]

The transactions take place through the real-time bidding process, where the ad exchange automatically receives offers of ad inventory in the form of bid requests from supplier websites via SSPs. Meanwhile marketers generally connect with the ad exchange through a DSP which indicates the maximum bid the marketer is will to make for certain types of ad inventory.

**Publisher ad servers** determine which advertisements to display to consumers on the various parts of the publisher's app or website, and when the advertisement will be displayed.[41] Publisher ad servers incorporate decision engines which place ads from external marketers, as well as determining which of the publisher's own internal promotions are displayed and when. In the case of the former, the publisher ad server may sit between the publisher and the SSP.

**Advertiser ad servers** provide creative management, store data about each advertising transaction and collect ad performance data.[42]

**Ad measurement, attribution and verification** services are provided to determine what a marketer must pay to the publisher for an advertisement (where that fee depends on the consumer's response to the advertisement), to verify that the advertisement was displayed according to the parties' contract and to determine the success of the advertisement.

**Measurement** vendors determine the types of audiences being reached by the advertisements and whether advertising campaign goals are being met.[43] Ad tech vendors also provide **verification** services to confirm that the marketer's advertisement was actually displayed on the agreed type of website at the agreed time.

Whereas in earlier years online advertisers paid "per impression" for their advertisements, it is increasingly common for advertising fees to be based on the subsequent actions of the consumer,[44] for example, whether the consumers clicks on the advertisement, or takes up a subscription with the marketer, or makes an online or offline purchase with the marketer.[45]

---

[39] See Chiradeep BasuMallick, 'What is an Ad Exchange? Definition, Functioning, Types and Examples' (Martech Advisor Online, 30 September 2019) https://www.martechadvisor.com/articles/ads/what-is-an-ad-exchange/?zd_source=mta&zd_campaign=8915&zd_term=chitraiyer , on the types of information exchanged and used by the DSP and SSP at the ad exchange.

[40] Alternatively, an advertising mediation platform might be integrated in the software of an app or website, creating a forum in which various ad networks compete for ad placements: Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 38. Ad exchanges are, eg, provided by OpenX, Rubicon Project, Yahoo Ad Exchange, Xandr, Google / Doubleclick Ad Exchange, Microsoft, SmartyAds.

[41] Examples of publisher ad servers include DoubleClick for Publishers, OpenX, AdButler, adzerk, Xandr and Facebook Audience Network.

[42] Examples of advertiser ad servers include Xandr, Sizmek, Google Ads and Facebook Ads.

[43] Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020), 24.

[44] See David S Evans, 'The Online Advertising Industry: Economics, Evolution, and Privacy' (2009) 23 *Journal of Economic Perspectives* 37, 38-39.

[45] Payment models include: CPM (cost per mille – cost per thousand impressions); CPC (cost per click); CPA (cost per acquisition); CPV (cost per view – video).

These payment models require further monitoring and tracking of the consumer's behaviour for **attribution** purposes to determine the advertising fee that must be paid. Datalicious by Equifax, for example, measures consumers' "granular user-level data in near-real time", online and offline, to attribute credit for sales to different elements of digital marketing.[46]

### 2.4 Major platforms: Google and Facebook

So far, this outline omits two of the most important players in the ad tech ecosystem. Google and Facebook are the two largest digital platforms operating in Australia and both firms depend on digital advertising for the vast majority of their revenue. However, as the Issues Paper notes, rather than relying on the services of various third-party ad tech vendors, these platforms integrate most of the functions outlined above within the businesses of one organisation.[47]

Google is by far the largest provider of online advertising and adtech services globally. For publishers, Google integrates the functions of an SSP, ad exchange and publisher ad server in one set of businesses. For marketers, Google integrates the functions of a DSP, data management platform, data analytics provider and advertiser in another set of businesses, which allows marketers to place advertisements on Google owned sites (such as Google Search, YouTube and Gmail) as well as third party publisher sites which sell ad inventory through Google.

Facebook's business model is different to Google's, but also highly integrated. For marketers, Facebook integrates the functions of a DSP, data management platform, data analytics provider and advertiser ad server in "Facebook Ads". Facebook Ads allows marketers to place advertisements on their choice of Facebook's own platforms (Facebook, Instagram and Messenger) as well as third party publisher websites that are part of the "Facebook Audience Network".[48] Facebook promises marketers that they can use the same "Facebook targeting" capabilities on its own platforms and these third party websites.[49] Facebook also essentially integrates the functions of an SSP, ad exchange and publisher ad server in its Facebook Audience Network, which places ads on third party publisher sites on behalf of those publishers in addition to placing advertisements on its own platforms.[50]

One of the many ways Google and Facebook have accumulated increasingly detailed and expansive personal data on consumers is by acquiring third-party ad tech vendors,[51] and merging the third-party vendors' consumer databases with the platform's own consumer database.[52]

Google and Facebook also constantly accumulate enormous quantities of personal data covering a wide range of the consumer's activities, via their numerous businesses operating in a broad range of markets. For Google, products include online search, video, email, education tools, data analytics, in-home

---

[46] See datalicious, 'Media Attribution' (datalicious website, accessed 23 April 2020) https://www.datalicious.com/our-services/media-attribution. See further 'Glossary' (datalicious website, accessed 23 April 2020) https://www.datalicious.com/resources/glossary#mta .

[47] ACCC, 'Ad Tech Inquiry Issues Paper' (10 March 2020) 22-23; Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 121-122.

[48] ACCC, 'Digital Platforms Inquiry: Final Report' (June 2019) 124, 128.

[49] See https://www.facebook.com/business/marketing/audience-network .

[50] ACCC, 'Digital Platforms Inquiry: Final Report' (June 2019) 124, 128.

[51] Some of which were noted by the ACCC, 'Ad Tech Inquiry: Issues Paper' (10 March 2020) 21, listing Google's acquisition of DoubleClick, AdMob and Adometry, and Taboola's acquisition of Outbrain. See further Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 22.

[52] See Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 22.

assistants, and digital advertising. For Facebook, products include social media, messaging, live streaming, photo sharing and digital advertising. Through their advertising customers (publishers and marketers), these companies also collect vast amounts of personal data which can be added to the existing profiles they have compiled on individual consumers.[53] Users do not have effective means to avoid this collection and combination of their personal data.[54]

Both Google and Facebook have frequently pointed out that they "do not sell" personal data, or only share it with other companies in very limited circumstances,[55] apparently as evidence of their respect for consumer privacy. However, while it is true that these platforms do not generally sell personal data, this should not be seen as ensuring individuals' privacy.

First, both Google and Facebook have suffered a number of major data breaches.[56] Based on this history, data stored by these firms is quite likely to be subject to improper use or access and suffer major data breaches in future. Concentrating data pools of unprecedented size and reach in the hands of a small number of large firms does not ensure the security of that data.

Second, Google and Facebook themselves can also use the personal data amassed on each individual against that individual's interests, including by increased data exposure, manipulative targeted marketing, and the potential for exclusion or discrimination.[57]

Third, Google and Facebook have both shown themselves determined to collect as much personal data as possible for commercial purposes, even if these data practices contradict the privacy preferences revealed

---

[53] The Facebook Data Policy (https://www.facebook.com/policy.php) states that:

> "Advertisers, app developers and publishers can send us information through Facebook Business Tools that they use, including our social plugins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about your activities off Facebook – including information about your device, websites you visit, purchases you make, the ads you see and how you use their services – whether or not you have a Facebook account or are logged in to Facebook. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its shop. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information."

The Google Privacy Policy (https://policies.google.com/privacy?hl=en-US) provides that:

> "We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf."

And later (https://policies.google.com/privacy/embedded?hl=en):

> "[A] website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your account settings, and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information."

[54] See Privacy International, 'No, Facebook is not telling you everything' (Privacy International website, 24 February 2020).

[55] The Facebook Data Policy states, "We don't sell any of your information to anyone and we never will." The Google Privacy Policy states, eg, "We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to."

[56] See, eg, Lily Hay Newman, 'A New Google+ Blunder Exposed Data from 52.5 Million Users' (Wired online, 12 October 2018); Emily Glazer, Tracy Ryan and Jeff Horwitz, 'Facebook Penalty is Set at $5 Billion' (The Wall Street Journal online, 13 July 2019); Josh Taylor, 'Facebook sued by Australian information watchdog over Cambridge Analytica-linked data breach' (The Guardian online, 9 March 2020); Darren Davidson and Dana McCauley, 'Zuckerberg protects his privacy, not ours' (The Australian online, 12 April 2018) regarding Facebook data breaches.

[57] See, eg, Alex Hern and Frederik Hugo Ledegaard, 'Children "interested in" gambling and alcohol, according to Facebook' (The Guardian online, 10 October 2019); Gautham Nagesh, 'Google on "Spy-Fi": We Failed Badly' (The Hill online, 22 October 2010).

by consumer surveys.[58] This personal data may be used for the platforms' behavioural and contextual advertising businesses, and/or to permit the platform to gain a competitive advantage in other markets or to enter new markets.

Importantly, while both platforms provide users with some capacity to opt out of receiving targeted advertising, they do not permit consumers to avoid the tracking of their online behaviour and the use and retention of that data for the platforms' other commercial purposes. In fact, both Google and Facebook constantly collect data on consumers who have no direct connection with Google or Facebook businesses in situations where the consumer is unlikely to be aware of this data collection.[59]

Amazon is another major digital platform, which may become increasingly significant in the ad tech sector. Aside from its position as the world's largest online retailer, Amazon has extended its operations to numerous other markets, including digital advertising. Amazon has amassed enormous quantities of consumers' personal data, including data from the operation of its online store and the Amazon Marketplace, a platform it provides for other merchants to sell their own products alongside Amazon products. The company has been criticised for using that data to advantage its own operations across markets, as well as allegedly advantaging sales of its own products at the expense of Amazon Marketplace merchants.[60]

Amazon does not yet enjoy a substantial share of digital advertising or ad tech services, but a number of factors make it likely to increase its presence in digital advertising in Australia, including the penetration of its businesses globally, its extensive datasets (particularly transaction data), its ability to link online data with growing search data from its in-home assistant "Alexa", and its competitive advantage in "proximity to point of purchase".[61] In marketing the services of the Amazon DSP, for example, the company promises marketers access to "Amazon audiences" across Amazon sites, apps and devices, as well as on third-party sites and apps, and a "full view of the customer journey from awareness to loyalty".[62]

### 2.5 Do ad tech businesses use "personal information"?

#### 2.5.1 Application of the Privacy Act to "personal information"

Many publishers, marketers and ad tech vendors claim that at least some of the data they use for marketing and behavioural advertising purposes is not "personal data" or "personal information".[63] These

---

[58] See ACCC, 'Digital Platforms Inquiry: Final Report' (June 2019) 379-381, on the growing volume and scope of data collected by Google and Facebook respectively.

[59] See, eg, Katharine Schwab, 'Google's reCAPTCHA has a dark side' (Fast Company online, 27 June 2019); Katharine Kemp, 'Australia's privacy watchdog is taking Facebook to court' (The Conversation online, 11 March 2020) regarding collection of non-user data on websites with a Facebook "Like" button or other Facebook technologies. The Google Privacy Policy ("your activity on other sites and apps" link) states:

> "Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your account settings, and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information."

[60] See, eg, Lina M Khan, 'Amazon's Antitrust Paradox' (2017) 126 *Yale Law Journal* 710, 780-783.

[61] Joseph Brookes, 'Prepare for the Digital "Triopoly" as Amazon's Advertising Model Emerges' (Which-50 online, 22 January 2019).

[62] Amazon Advertising: https://advertising.amazon.com.au/products/amazon-dsp?ref_=a20m_au_fnav_dsp

[63] See Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 133. See, eg, the Sizmek by Amazon Privacy Policy (https://www.sizmek.com/privacy-policy/) which states:

firms often state that the relevant data has been "de-identified" or "anonymised" such that it is no longer personal information. The implication is that use of this data poses no risk to the consumer and/or is not governed by the Australian Privacy Principles (APPs) under the *Privacy Act*, such that the firm may use it for any purpose whatsoever.[64]

These claims should be carefully scrutinised. At the outset, there are strong arguments that de-identification efforts are increasingly ineffective.[65] In the ad tech context, there is the question of whether the relevant data does, or should, fall within the definition of "personal information", given its association with a unique person.

The *Privacy Act* imposes obligations on "APP entities".

Most firms described in sections 2.3 and 2.4 above are likely to come within the definition of an "APP entity", since, in most cases, the firm:

- has annual revenue over AUD 3 million in the previous financial year, or
- "discloses personal information about another individual to anyone else for a benefit, service or advantage", or
- "provides a benefit, service or advantage to collect personal information about another individual from anyone else".[66]

Under the Act, "personal information" means:

> *information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
> *(a) whether the information or opinion is true or not; and*
> *(b) whether the information or opinion is recorded in a material form or not.*[67]

The term "de-identified" is also defined. According to the Act, "personal information is ***de-identified*** if the information is no longer about an identifiable individual or an individual who is reasonably identifiable".[68]

---

> "The information we collect is associated with your cookie identifiers and/or mobile advertising identifiers (if you are using a mobile device), as well as your IP address. We never collect information about your actual identity. …
>
> [O]ur technology employs cookies, device identifiers and similar technologies (like pixels and statistical device identifiers) to collect information about your browser or device, the sites it has visited and the apps it has used, the advertisements served to it, interactions with those advertisements, and, where available, the approximate geographic location of the device ("ad serving information"). …
>
> This ad serving information, which does not enable Sizmek to determine your actual identity, may be shared with our customers and Sizmek's and our customers' partners for our customers' advertising purposes."

[64] See, eg, The Australian Financial Review Privacy Policy (https://www.afr.com/privacy-policy) :

> "We may also collect anonymous data (which is not personal information) relating to your activity on our websites (including IP addresses) via cookies, or we may collect information from you in response to a survey. We generally use this information to report statistics, analyse trends, administer our services, diagnose problems and target and improve the quality of our products and services. To the extent this information does not constitute personal information because it does not identify you or anyone else, **the Australian Privacy Principles do not apply and we may use this information for any purpose and by and [sic] means whatsoever**." (emphasis added)

[65] See, eg, Chris Culnane and Kobi Leins, 'Misconceptions in Privacy Protection and Regulation' (2019) 36 *Law in Context* (forthcoming).

[66] Privacy Act, s 6D.

[67] Privacy Act, s 6(1).

[68] Privacy Act, s 6(1).

The critical question for publishers, marketers and ad tech businesses will often be whether the information or opinion is "about an identified individual or an individual who is reasonably identifiable". These concepts currently lack clarity under Australian law.

### 2.5.2 "De-identified" data, unique identifiers, ID syncing and resolution

Firms stating that certain of their data practices only involve "de-identified", "anonymised" or "aggregated" data imply that this data is not about an identified individual or an individual who is reasonably identifiable.[69] It is clear, however, that many businesses aim to distinguish, profile and interact with individual consumers by using "de-identified" data. They often achieve this objective by using "unique identifiers", that is, unique strings of numbers and/or letters that are assigned to a particular device or individual in the absence of a name or email address.[70]

Unique identifiers intended to track a consumer's activity include identifiers derived from email addresses (such as "hashed" email addresses); cookie identifiers; device identifiers; IP addresses; and advertising identifiers (such as the Android Advertising ID).

These are not random identifiers dissociated from any actual individual. On the contrary, these identifiers are intended to permit firms to associate information across devices, companies, services and transactions with a particular individual, whether or not that individual is identified by name.[71] Ad tech businesses often refer to this as "people-based marketing".[72]

This profiling of a given individual is given a very high priority in the ad tech industry. The Interactive Advertising Bureau (IAB) is a trade association for online advertising, with 43 offices globally including an office in Australia.[73] The IAB advises its members that:[74]

> *In order to deliver truly personalized and relevant messaging, marketers should not only work with cross-device identity vendors, but also with attribution providers and internal data teams to help them* ***not just connect and match devices with unique, people based IDs, but also to gain an understanding of the consumer behind the device****.*

---

[69] The Google Privacy Policy (https://policies.google.com/privacy?hl=en-US) appears to imply that it does not regard information tied to a unique identifier as personal information, but it fails to clarify this. It states:

> "When you're not signed in to a Google Account, we store the information that we collect with unique identifiers tied to the browser, application or device you're using. …
>
> When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information."

[70] Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 25.

[71] Jessica Davies, 'Shared Identity Solutions' (Digiday online, 23 September 2019) https://digiday.com/media/what-are-shared-identity-solutions-and-can-they-really-replace-cookies/ explains that "shared-ID consortiums and businesses" are "working on shared versions, meaning the creation of one (anonymous) unified ID per individual that publishers and their programmatic ad partners can use to serve and target ads".

[72] See, eg, Goodway Group, 'What is People-Based Marketing?' (Goodway Group website, accessed 23 April 2020) https://goodwaygroup.com/blog/what-is-people-based-marketing/:

> "At the most basic level, people-based marketing means gathering customer data from both offline and online sources and using that rich profile to more accurately recognize and reach customers on any device."

[73] "About IAB" (IAB Australia website) https://www.iabaustralia.com.au/about-iab-australia/about-iab .

[74] IAB, 'Mobile Identity Guide for Marketers: A Best Practices Primer for Mobile & Cross-Device Marketing' (IAB, 2017) 12 https://www.iab.com/wp-content/uploads/2017/06/Mobile-Identity-Guide-for-Marketers-Report.pdf (emphasis added).

Mathieu Roche, CEO of "shared ID" provider ID5, has stated: [75]

> *An ID is a key in a database. It is* ***the first bit of code that you can attach all you know about the user to, but it has to be unique****. The purpose is for the same ID to be shared between publishers and brands — it has to be the same key. It is a common language for ad tech*.

To achieve this, some suppliers aim to "resolve" or "sync" the details of each consumer across different databases, devices and services, to permit firms to recognise and track the individual consumer without reference to their name or email address. These services may take the form of "cookie syncing" (linking information from cookies placed on the consumer's device by different firms) or "ID syncing" (linking different identifiers assigned to the same consumer).[76]

LiveRamp promises that with its IdentityLink services it can:[77]

> *[c]reate targeted, people-based campaigns by* ***resolving first-, second-, third-party data to a single unique identifier*** *that can be onboarded to 500+ destinations through the LiveRamp platform for omnichannel targeting, measurement, and analytics across digital and TV.*

Adobe describes its "ID synchronization" process as follows:[78]

> *ID synchronization matches IDs assigned by the ID service to IDs assigned to site visitors by our customers. For example, say the ID service has assigned a visitor ID 1234. Another platform knows this visitor by ID 4321. The ID service maps these IDs together during the synchronization process. The results add new data points to what our customers know about their site visitors. And, if the ID service can't match an ID, it creates a new one and uses that ID for future synchronization.*

Claims that publishers, marketers and ad tech vendors exchange only non-personal information should be carefully scrutinised. As Culnane and Leins point out, an individual may be even more accurately identifiable by their behavioural and device data than by their given name:[79]

> *The data points that represent that individual's actions, devices, location, etc are often as effective, if not more effective, at identifying an individual as traditional identifiers …*

There can be no doubt that these strategies aim to address a single individual and to combine data about that individual from numerous databases to create an individual profile, even if that profile is not attached to individual's actual name or email address. Singled out in this way, the individual can be subjected to growing risks of re-identification, manipulation, exclusion and discrimination.

### 2.5.3 Legislative clarification in line with ACCC recommendation

Traditionally, an individual would be identified by their given name, combined with some other information such as a postal address, email address, employment position or family connection. However, the outline

---

[75] Jessica Davies, 'Shared Identity Solutions' (Digiday online, 23 September 2019) https://digiday.com/media/what-are-shared-identity-solutions-and-can-they-really-replace-cookies/ (emphasis added).

[76] Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 27.

[77] 'Introducing LiveRamp IdentityLink' (LiveRamp website) https://liveramp.com/blog/introducing-liveramp-identitylink/ (emphasis added).

[78] 'Understanding ID synchronization and match rates' (Adobe website) https://docs.adobe.com/content/help/en/id-service/using/intro/match-rates.html .

[79] Chris Culnane and Kobi Leins, 'Misconceptions in Privacy Protection and Regulation' (2019) 36 *Law in Context* (forthcoming).

above indicates that online businesses frequently seek to single out an individual without reference to these traditional identifiers.

The concept of identification should not be limited to data which is labelled with a consumer's legal name or contact details, but should extend to data which can be used to single out one consumer as distinct from other consumers.

The UK ICO has recognised that an individual may be identifiable "either as a named individual or simply as a unique user of electronic communications and other internet services who may be distinguished from other users".[80]

The Australian case law on the meaning of "personal information" does not currently provide this clarity. In *Privacy Commissioner v Telstra Corporation Ltd*,[81] the Full Federal Court upheld the decision of the Administrative Appeals Tribunal (AAT) on the narrow issue that personal information must be "about an individual" and that those statutory words should be given substantive effect.[82] The case concerned mobile network "metadata",[83] including Internet Protocol (IP) addresses, recorded and stored by Telstra.

The Deputy President of the AAT had concluded that the IP addresses allocated to a mobile device which the individual complainant used were not "about" that individual since "an IP address is not allocated exclusively to a particular mobile device".[84] The Full Federal Court noted the Deputy President's conclusion that:

> *The IP address might even change frequently in the course of a communication. For that reason, the Deputy President concluded that the connection between the person using a mobile device and an IP address was too ephemeral for the IP address to be 'about' the individual. Instead, it was about the means by which data is transmitted from a person's mobile device over the internet and a message sent to, or a connection made, with another person's mobile device.*[85]

However, the appeal to the Full Federal Court did not concern this finding and accordingly the Court reached no conclusion of its own in this respect.[86] The Court did not consider the question of when various metadata could in fact constitute "personal information".[87]

In the DPI Final Report, the ACCC recommended that the definition of "personal information" under the Privacy Act should be updated "to clarify that it captures data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual".[88] The ACCC recommended in particular that the definition should be amended to reflect the wording of the GDPR, bringing the added benefit of alignment with international standards.[89]

---

[80] UK ICO, 'What are identifiers and related factors?' (UK ICO website) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/ .

[81] [2017] FCAFC 4, para 5, 73.

[82] [2017] FCAFC 4, para 80.

[83] Essentially, "data that provides information about data": [2017] FCAFC 4, para 5.

[84] [2017] FCAFC 4, para 44.

[85] [2017] FCAFC 4, para 44.

[86] [2017] FCAFC 4, para 44.

[87] [2017] FCAFC 4, para 73.

[88] ACCC, 'Digital Platforms Inquiry: Final Report' (June 2019) 458.

[89] ACCC, 'Digital Platforms Inquiry: Final Report' (June 2019) 458.

The GDPR recognises that a name is only one way that a person can be identified. Various online identifiers may equally identify an individual. Article 4(1) of the General Data Protection Regulation (GDPR) specifies that:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject')".*

The definition proceeds to clarify that:

> *an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

Recital 30 expands on the relevance of online identifiers:

> *Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.*

Under the GDPR, therefore, unique identifiers can constitute personal data.[90]

The use of strategies which single out unique individuals and create a detailed picture of "the consumer behind the device", alongside the claim that these practices involve no personal information, exposes consumers to growing risks of re-identification, manipulation, exclusion and discrimination.

This adds weight to the ACCC's recommendation in the DPI Final Report that the Privacy Act should be amended to clarify, in line with the GDPR, that "personal information" includes "data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual".

### 2.5.4 The underwhelming death of the third party cookie

There has been a further development in the online identification of consumers over the last few years, driven largely by developments in online browsers. Responding to consumers' privacy concerns,[91] Apple and Firefox introduced online browsers with privacy settings which enabled consumers to block all or most third party cookies.[92]

Cookies are small text files placed on a consumer's device which allow the originator of the cookie to retrieve information about the consumer which is stored in that text file over time. If, while a consumer is

---

[90] See Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 25. In the United States, on the other hand, unique identifiers are not treated as "personally identifiable information": at 98.

[91] Kristina Monllos, '"They've started to render DMPs useless": Omnicon Media Group CEO Scott Hagedorn's State of Programmatic Advertising' (Digiday online, 8 May 2019):

> "Everyone was rushing toward a reality where we could have a central nervous system and DSP and a [data management platform] that was plugged in the multiple DSPs and multiple ecosystems. That was going to be the future of behavioral media and the future of advertising. And then there's a privacy backlash and people being like, "Well, how exactly do you know that I was here on another screen and now they're on this one? How is my data being utilized?""

[92] See Gerrit de Vynck, 'Firefox follows Apple in blocking third-party cookies online' (Bloomberg online, 4 June 2019); Nick Statt, 'Apple updates Safari's anti-tracking tech with full third-party cookie blocking' (The Verge online, 24 March 2020).

visiting a website, the operator of that website places a cookie on the consumer's device, that is regarded as a first party cookie. If, while the consumer is visiting that website, some other party places a cookie on the consumer's device, that is considered to be a third-party cookie. These are also referred to as "tracking" or "targeting" cookies.

Many of these third party cookies are placed on consumers' devices for the purpose of identifying an individual consumer between websites and providers, adding to that consumer's profile across providers and displaying targeted advertising to the consumer.

Many publishers and marketers saw the blocking of third party cookies by Apple and Firefox browsers as problematic, claiming that, without identification via third party cookies, advertising opportunities and therefore advertising revenue decreased.[93] This concern greatly increased in January 2020, when Google announced that it would be disallowing third party cookies on its Chrome browser from 2022.[94]

However, the "death of the third party cookie" cannot be regarded as an overwhelming victory for consumer privacy for a number of reasons.

First, while Google's announcement was the most substantial development, given the company's size and market share, Google has only resolved to remove third party cookies. The firm has made no suggestion that it will stop tracking consumers itself via its own websites and apps, or combining that data with data it collects via the first party cookies of its publisher and marketer clients.[95] This means consumers will continue to be pervasively monitored, if by a smaller number of more powerful firms.

Second, publishers, marketers and ad tech businesses have a number of other means of identifying consumers even in the absence of third party cookies. Numerous players propose to rely more heavily on their own first party cookies as well as "registration walls", that is, requiring consumers to register and login to use their sites.[96] This will allow the firm to track activity of individual consumers via that login identification, and increase their first party data.[97] Some publishers have moved to form more "data partnerships", by reaching agreements to disclose first party personal data about their own customers in exchange for second party data, that is, personal data about the other firm's customers.[98]

Beyond this expansion of first- and second-party data, there are numerous ways to identify consumers across different devices and websites even in the absence of third-party cookies. These include "device fingerprinting",[99] as well as the use of persistent advertising identifiers such as Apple's Identifier for

---

[93] See Ariel Bogle, 'Google wants to kill third-party cookies: Here's why that could be messy' (ABC online, 21 January 2020).

[94] Justin Schuh, 'Building a more private web: A path towards making third party cookies obsolete' (Chromium blog, 14 January 2020) https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html?mod=article_inline ; Bowdeya Tweh and Sahil Patel, 'Google Chrome to Phase Out Third-Party Cookies in Effort to Boost Privacy' (The Wall Street Journal online, 14 January 2020); Nat Ives, 'Marketers and Ad Agencies Ask Google Not to Kill Cookies Too Soon' (The Wall Street Journal online, 16 January 2020).

[95] Ariel Bogle, 'Google wants to kill third-party cookies: Here's why that could be messy' (ABC online, 21 January 2020); Seb Joseph, 'Winners, losers and fallout from Google's plan to drop cookies' (Digiday online, 16 January 2020).

[96] Tim Peterson, 'The industry is looking to first-party data to replace cookies, but the open web may lose out' (13 February 2020) on the threats to the "open web" from the "registration wall" approach.

[97] This also has the advantage for the publisher of establishing deterministic identity, rather than probabilistic identity, for targeted advertising and attribution.

[98] See Lucinda Southern, '"The Google doomsday clock is ticking": Publishers scramble to benefit from post-third-party cookie data partnerships' (Digiday online, 26 February 2020).

[99] "Device fingerprinting" refers to the process of using a set of information to "single out, link or infer a user, user agent or device over time": Article 29 Data Protection Working Party, 'Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting' (25 November 2014) 4.

Advertising and Google's Android Advertising ID.[100] Still more argue that diverse customer records can now be matched using machine learning in the absence of these identifiers.[101]

There are also proposals to adopt a universal, unique identifier for each consumer which would be broadcast to ad tech firms, but which might permit consumers to make privacy choices (other than not having a unique identifier apparently).[102]

In short, in response to efforts to block pervasive tracking of consumers by third party cookies, many firms have simply begun to establish other ways to persistently identify and track consumers, rather than permitting consumers to choose not to be persistently identified in their online activities.

## 2.6 Consumer consent to data practices

### 2.6.1 Notice and consent requirements under the Privacy Act

One of the justifications firms raise for the data practices explained above is that consumers have been notified of these data practices via the relevant firms' privacy policies and that consumers have at least impliedly consented to these practices since the firms provide a link to their privacy policies on their respective websites. These justifications are based on notice and consent obligations under the APPs established by the Privacy Act.

APP entities must notify individuals that personal information about them has or will be collected.[103] APP entities must also publish a "clearly expressed and up to date" privacy policy "about the management of personal information by the entity".[104] These privacy policies must include notice about what kinds of personal information the entity collects, how the entity collects and holds that information and the purposes for which they use and disclose it, among other things.[105]

Further, an APP entity must not engage in certain activities unless the relevant individual consents, including:

- collecting sensitive information about an individual;[106]
- using or disclosing personal information for a purpose other than the particular purpose for which it was collected;[107]
- using or disclosing sensitive information about an individual for the purpose of direct marketing;[108] and

---

[100] IAB, 'Mobile Identity Guide for Marketers: A Best Practices Primer for Mobile & Cross-Device Marketing' (IAB, 2017) 4 https://www.iab.com/wp-content/uploads/2017/06/Mobile-Identity-Guide-for-Marketers-Report.pdf .

[101] Eg, data analyst, Amperity, explains in "What We Do" (Amperity website) https://amperity.com/what-we-do/data-foundation:

> "Amperity applies a patented machine learning-powered approach to accurately and comprehensively unify records from every system, even when records lack an email address, phone number, loyalty number, or other traditional identity marker."

[102] See Paige Murphy, 'Industry reacts: Experts welcome Google Chrome's third-party cookie removal' (AdNews online, 24 January 2020) https://www.adnews.com.au/news/industry-reacts-experts-welcome-google-chrome-s-third-party-cookie-removal .

[103] APP 5.

[104] APP 1.3.

[105] APP 1.4.

[106] With some exceptions, APP 3.3.

[107] With some exceptions, APP 6.1.

[108] APP 7.4.

- disclosing personal information to an overseas recipient.[109]

There is no comprehensive definition of "consent" under the Privacy Act. The Act only states that "consent" means "express consent or implied consent".[110] The OAIC has published non-binding Australian Privacy Principles Guidelines which include guidance on appropriate standards for consent.

### 2.6.2 Purported notice and consent under existing privacy policies

The OAIC identifies four key elements of consent in its Guidelines as followed:

- the individual is adequately informed before giving consent;
- the individual gives consent voluntarily;
- the consent is current and specific; and
- the individual has the capacity to understand and communicate their consent.

In many cases, the consents to consumer profiling and ad tech uses of personal data alleged by the firms described in this article fall short of the standards recommended by the OAIC.

***"Bundled" consent is not voluntary***

Consumer consent should not be regarded as voluntary where it is obtained by the bundling of consents for different uses and purposes in the relevant privacy policy. Nonetheless, in the case of publishers' and marketers' privacy policies, the firm's notice about data practices necessary for the firm to provide the relevant service to the consumer almost universally includes purported consents for other broad marketing purposes, with no provision for the consumer to consent to one and refuse the other.

For example, a major bank might provide a privacy policy which states that it will use the consumer's personal information to supply the consumer with financial services as well as disclosing that personal information to a broad category of third parties who "share information for marketing purposes",[111] without providing any options in this respect.

Similarly, a consumer purchasing a subscription to 'The Australian' newspaper is required to accept the 'News Corp Australia Privacy Policy' which provides in part that:[112]

> *We may combine information that we hold about you with information about you that we collect from other trusted businesses with whom you also have a relationship or from public sources and we may associate your browser and/or device with other browsers or devices you use. We may also share information we hold about you with those trusted businesses so that they can do the same thing.*

---

[109] If certain further conditions are met: APP 8.2.

[110] Privacy Act, s 6(1).

[111] See, eg, NAB Privacy Policy https://www.nab.com.au/content/dam/nabrwd/documents/policy/banking/nab-privacy-policy.pdf :

"We may disclose your personal information to third parties outside of the Group, including: …

- organisations we sponsor and loyalty program partners, including organisations the NAB Group has an arrangement with to jointly offer products or has an alliance with to share information for marketing purposes;"

[112] News Corp Australia Privacy Policy (https://preferences.news.com.au/privacy).

Consent to such broad, unrelated purposes should not be regarded as voluntary where it is bundled with the primary purpose in this way.

***Vague, open-ended and incomplete privacy policies do not adequately inform***

Publishers, marketers and data brokers often claim consumers consent to the use of their data for additional purposes relating to marketing or commercial data sharing arrangements on the basis of vague, open-ended terms in privacy policies.

The relevant terms are often phrased in a way that the consumer cannot determine the actual uses of the personal data and the entities to whom that data will be disclosed. The terms used are entirely open-ended. For example, the publisher, Fairfax Media Ltd, states in 'The Australian Financial Review Privacy Policy':[113]

> *We may disclose your personal information to: … our existing or potential agents and/or business partners …*

The Policy does not identify or limit the entities that might fall within these categories.

Google has for a number of years provided its reCAPTCHA security product to a large number of publisher websites worldwide, including businesses in Australia. The reCAPTCHA badge displayed on these websites is underscored by a small link titled "Privacy". Following that link will take the consumer to the general Google Privacy Policy. Although reCAPTCHA collects a range of data about the consumer's device and activity on websites,[114] the Google Privacy Policy makes no mention of the reCAPTCHA product or the data practices associated with it.

The privacy policy for the publisher TikTok, a popular social media app, states:[115]

> *We also share your information with business partners, other companies in the same group as TikTok Inc, content moderation services, measurement providers, advertisers and analytics providers.*

The TikTok Privacy Policy does not list or limit the advertisers, measurement providers or analytics providers to whom users' personal information can be disclosed.

As the Norwegian Consumer Council pointed out in its report on the privacy policies and data practices of popular mobile apps, consumers "have no way of knowing which entities process their data and how to stop them".[116] The UK ICO has noted that the transfer of consumer's personal data to numerous third party vendors gives rise to a very significant risk that the data will be improperly stored and used, particularly since the original collector of the data no longer has control over it.[117]

---

[113] The Australian Financial Review Privacy Policy (https://www.afr.com/privacy-policy)

[114] On these uses, see Katharine Schwab, 'Google's reCAPTCHA has a dark side' (Fast Company online, 27 June 2019).

[115] TikTok Privacy Policy (https://www.tiktok.com/legal/privacy-policy?lang=en).

[116] Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 6.

[117] Information Commissioner's Office, United Kingdom, 'Update Report into Adtech and Real Time Bidding' (Report, 20 June 2019) 20-21.

***Consent received via numerous or unidentified third parties is insufficient***

The effect of these inadequately informed, bundled consents snowballs as third parties in the ad tech supply chain in turn rely on these broad permissions as consent for their own data practices.

Numerous privacy policies include terms intended to provide permission for the firm to receive the consumer's personal data from third parties and combine it with the firm's first party data about that consumer. Again, the consumer is not provided with options in this respect.[118]

The Woolworths Rewards "Collection Notice" states:[119]

> *We collect personal information about Woolworths Rewards Members from other persons or entities. For example, we collect personal information for marketing purposes from other suppliers of goods or services who, like us, have an existing relationship with Woolworths Rewards Members. …*

The Amazon "Cookies & Internet Advertising" policy states:[120]

> *Also, some third-parties may provide us information about you (such as demographic information or sites where you have been shown ads) from offline and online sources that we may use to provide you more relevant and useful advertising.*

The NAB Privacy Policy contains a similar statement:[121]

> *We may* ***use or disclose information about you in order to combine the information that we hold with information collected from or held by external sources****. We do this in order to enable the development of customer insights about you so that we can serve you better.*

Other major banks include similar terms in their privacy policies.[122]

In each of the above cases, the consumer is provided with no option to decline this collection and combination of their personal data with data from other suppliers and third parties, which is not necessary for the provision of the relevant service.[123]

---

[118] Eg, the Google Privacy Policy states (https://policies.google.com/privacy?hl=en-US):

> "We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf."

[119] Woolworths Rewards Collection Notice: https://www.woolworthsrewards.com.au/collection-notice.html

[120] Amazon "Cookies & Internet Advertising": https://www.amazon.com.au/gp/help/customer/display.html?nodeId=201380490

[121] NAB Privacy Policy: https://www.nab.com.au/content/dam/nabrwd/documents/policy/banking/nab-privacy-policy.pdf (emphasis added)

[122] Eg, the Commonwealth Bank of Australia Privacy Policy states (https://www.commbank.com.au/content/dam/commbank/security-privacy/privacy-policy.pdf):

> "New technologies let us **combine information we have about you** and our other customers, **for example transaction information, with data from other sources, such as third party websites** or the Australian Bureau of Statistics. We analyse this data to learn more about you and other customers …" (emphasis added)

[123] While the consumer may be able to opt out of receiving targeted advertising, they are not given the option of avoiding the collection and combination of their personal data from third parties.

It appears that ad tech vendors, data brokers, data aggregators, data analytics providers and data management platforms also rely on such broadly worded, take-it-or-leave-it terms in the privacy policies of their clients as evidence of consumers' consent to data sharing facilitated by their services.[124]

Further, firms often rely on the validity of third-party privacy policies to justify their data practices, while disclaiming responsibility for those policies and requiring consumers to identify and analyse those policies for themselves. For example, the TikTok Privacy Policy states:[125]

> *Additionally, we allow these service providers and business partners to collect information about your online activities through Cookies. We and our service providers and business partners link your contact or subscriber information with your activity on our Platform across all your devices, using your email or other log-in or device information.* ***Our service providers and business partners may use this information*** *to display advertisements on our Platform and elsewhere online and across your devices tailored to your interests, preferences, and characteristics.* ***We are not responsible for the privacy practices of these service providers and business partners****, and the information practices of these service providers and business partners are not covered by this Privacy Policy.*

Similarly, the privacy policy for the flybuys retail loyalty scheme states that customers should review the privacy policies of various third parties in respect of certain data "sharing" arrangements, without specifying who those third parties are:[126]

> *In addition to this Privacy Policy, our Participants, Coles, and Wesfarmers group companies have their own privacy statements and other terms which provide further information about the handling of your Personal Information that has been shared with these parties.* ***We are not responsible for the privacy practices of policies of these third parties and recommend that you review their respective privacy policies.***

Such empty injunctions to read unspecified third party privacy policies should not be treated as valid consent to these practices, nor absolve the firm of responsibility for these data disclosures.

***Ineffective opt-outs and device settings do not indicate consent***

In some instances, the privacy policies of websites or apps state that consumers can choose to opt out of certain tracking or the acceptance of cookies, by changing their device settings. Implicitly, in the absence of taking this action, consumers are allegedly consenting to the firm's tracking activities. However, attempts to make use of opt outs and device settings often have very little effect.[127]

Critically, many of the opt outs do not permit the consumer to choose not to have their behaviour tracked, monitored and recorded, but only to opt out of *receiving* targeted advertising on the basis of that personal data.[128] Consumers should have the option not to have their behaviour tracked, monitored and recorded for

---

[124] Consider, eg, Data Republic Privacy Policy: "We may disclose personal information for the purposes described in this privacy policy to: … specific third parties authorised by you to receive information held by us".

[125] TikTok Privacy Policy (https://www.tiktok.com/legal/privacy-policy?lang=en) (emphasis added).

[126] flybuys Privacy Policy (https://www.flybuys.com.au/about#/privacy-policy) (emphasis added). See also MoPub privacy policy, referring to over 160 partners; and Smaato listing more than 1000 partners: Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 159.

[127] Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 69, 179.

[128] ACCC, 'Customer Loyalty Schemes: Final Report' (December 2019) 74-75.

purposes beyond that which is necessary for the provision of the immediate service. In fact, the default position should be that they are not tracked in this way.

In other instances, opting out requires complex, time-consuming and repeated action on the part of the consumer, which, even then, cannot produce a complete avoidance of tracking for marketing purposes.[129] For example, Sizmek by Amazon, an ad server, provides a 'Cookie Consent Tool' which states:[130]

> *We use the following partners to better improve your overall web browsing experience. They use cookies and other mechanisms to connect you with your social networks and tailor advertising to better match your interests. You can elect to opt-out of this information collection by unticking the boxes below.*

The page lists 22 such "partners" by name, including DSPs, ad exchanges, analytics providers and data aggregators. Following Sizmek's instruction to opt out by "unticking the boxes below" and click on the "Opt Out All" button produces the message "Opting out … Opted out". However, a closer look at the faint type against the subsequent list of partners reveals that only 7 partners' cookies are thereby disabled. Of the balance, 4 partners are labelled "this partner does not provide a cookie opt out" and 11 more are labelled "opt out through company".

Other privacy policies provide that if consumers do, for example, turn off the location-based tracking or GPS on their device, the app can still infer the consumer's location by using other data, including IP address, Wi-Fi access point information, Bluetooth, and cell tower data.[131]

Similarly, when consumers who are members of the flybuys and Woolworths Rewards retail loyalty schemes choose not to scan their loyalty cards for a particular purchase, the flybuys and Woolworths automatically link their payment card to the consumer's membership profile regardless.[132] Neither flybuys or Woolworths Rewards have amended their privacy terms in this respect, in spite of the ACCC's call for them to desist. Accordingly, a customer may believe they have stopped using their loyalty card and therefore avoided ongoing tracking, while the firm continues to track them through their payment cards.

### 2.6.3 Legislative reform in line with ACCC recommendations

The OAIC Guidelines were originally published in 2014.[133] However, it is clear from the prevalence of the terms described above that these non-binding guidelines have not deterred firms from relying on "consents" which fall well short of the standards outlined by the OAIC.

In the DPI Final Report, the ACCC recommended that the requirement for consent should be extended to "whenever a consumer's personal information is collected, used or disclosed by an APP entity", with certain

---

[129] See, eg, the description of ineffectual opting out via www.youronlinechoices.com.au in ACCC, 'Customer Loyalty Schemes: Final Report' (December 2019) 69, 74-75.

[130] See Sizmek by Amazon website (https://www.sizmek.com/).

[131] Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 105, 128. At 83:

> "This means that, even if a consumer explicitly turns off the GPS function on their smartphone, their location can be accurately triangulated by third parties through measuring the phone signal and distance to Wi-Fi access points and cell towers."

[132] ACCC, 'Customer Loyalty Schemes: Final Report' (December 2019) 65-67.

[133] The current version is version 1.3. However, the guidance referred to in this article took the same form in the original version in 2014.

limited exceptions.[134] The ACCC also recommended that "[v]alid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent)".[135] It noted that this amendment would be "in line with the higher standard of data protection provided under the GDPR".[136]

"Consent" is one of the six possible lawful grounds for processing personal data under the GDPR.[137] The GDPR sets standards for consent that overlap with the OAIC guidelines to some extent.

"Consent" is defined under article 4 of the GDPR, which states that:

> *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*

Further, Article 7 of the GDPR clarifies that:

> *When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

Accordingly, under the GDPR, a firm cannot argue that a consumer consented to the processing of personal data where performance of a contract was conditional on the consumer providing consent to data processing that was not necessary for the performance of the contract. So, for example, where a bank bundles consent to data practices necessary for the provision of the relevant financial services with consent to use of the data for "marketing and research", the alleged consent to this latter use would not be valid.

The GDPR definition is given further content in the recitals to the GDPR, including Recital 32, which states in part:

> *Silence, pre-ticked boxes or inactivity should not therefore constitute consent.*

Under the GDPR, therefore, the "implied consent" currently recognised under the *Privacy Act* would not constitute valid consent. Inactivity should not suffice. Consumers should not be required to navigate multiple, deliberately complex "opt out" procedures, nor perform the Sisyphean task of maintaining their choice not to be tracked against constantly evolving technologies designed to circumvent that choice. In the absence of action by the consumer, default settings should favour privacy.

The trends in privacy policies outlined above make the claims that consumers have consented to the privacy-degrading data practices of the ad tech sector spurious, often disingenuous. The adoption of the ACCC recommendations on notice and consent in the DPI Final Report are vital first steps in ensuring that publishers, markets and ad tech vendors do not rely on fictional consents to justify their data practices.

---

[134] ACCC, 'Digital Platforms Inquiry: Final Report' (June 2019) 464.

[135] ACCC, 'Digital Platforms Inquiry: Final Report' (June 2019) 464.

[136] ACCC, 'Digital Platforms Inquiry: Final Report' (June 2019) 466.

[137] GDPR, Article 6(1).

## Conclusion

The ad tech sector is founded on consumers' personal data. Technological advances have provided growing opportunities for firms to profit by predicting, prompting, and measuring consumers' behaviour on a daily basis. This has led publishers, marketers and ad tech service providers to increasingly monitor and track individuals online and offline in the service of consumer profiling, behavioural advertising and attribution of consumer responses.

Realising that this extensive collection and use of personal data is against the preferences of many consumers, firms have taken measures to make this data collection less visible, to obfuscate their data practices in opaque privacy policies, to create the illusion of consumer control and choice where little exists, and to circumvent consumers' attempts to avoid the collection of their personal data and monitoring of their behaviour.

In advertising markets, ad tech vendors provide highly sophisticated algorithmic tools and instantaneous auction processes. These give the appearance of almost frictionless allocation of available advertising inventory to marketers who value it the most. However, in addition to the many distortions that arise in those processes, the analysis of competition in these markets should take into account the fundamental distortion that results from the anticompetitive and consumer-harming data practices in the primary markets in which that data is collected.