KINESSO

Chrome's Curtain Call for Cookies:

Everything you need to know, a marketers guide to privacy changes.

Introduction.

The media landscape is going through fundamental shifts with the impending deprecation of 3rd party cookies in Chrome, now in 2025, and Privacy Legislation changes with confirmation the proposed legislation will be introduced in the House of Representatives in August 2024.

While these two events are independent, they are intrinsically linked as the need for privacy change is largely being driven by three factors:

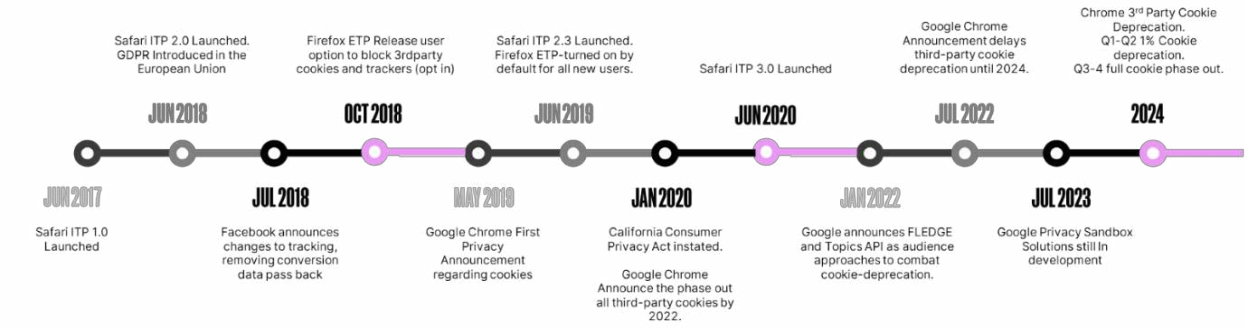
- **Consumer demand:** consumers are rightfully becoming more protective of the currency of their online data. While still expecting personalised experiences, consent management puts the power in the consumers hands to consent to brands they trust. The Government run CAPS survey found that 84% of Australians want more control and choice over the collection and use of their personal information.
- **Regulation:** with reforms occurring around the globe (GDPR in Europe and CCPA in California), the Australian Government has had to fast-track privacy reform in this market, and this reform will shape the way the advertising industry collects and uses data in the future.
- **Technology:** changes to traditionally used identifiers such as 3rd party cookies and device IDs, in certain environments, has prompted a new approach to how we buy and measure advertising and prompted the rise of new privacy safe ID solutions and aggregated audience solutions.

Changes are coming.

While the deprecation of 3rd party cookies is by no means a new concept to the industry (Safari and Firefox began phasing out cookies back in 2013 and have already completed the total deprecation of 3rd party cookies), it is important to note that the change in Chrome will be significant due to the incredibly large market share the browser holds in Australia (52%).

Considering that, if 90% of your target audience uses an Apple device, then your agency partner would have already been addressing your wastage and reporting crisis for the

past 24 months. If they have not, and your audience is predominantly in that 52% of Chrome browser users, then read on.



It's important to make the distinction between 1st and 3rd party cookies, as the deprecation is only occurring across 3rd party cookies.

1st party cookies are a cookie placed on a user's browser by the webpage they are visiting. These cookies are used so the site can remember login details, payment information and will remain intact for targeted advertising by a brand.

A 3rd party cookie is a cookie placed on a user's browser by a third party i.e. not the webpage they are visiting. These cookies are used to track a user's behaviour across the internet for the purpose of anonymous visitor recognition, conversions and most commonly for cross-site and cross-channel tracking for personalised advertising.

Google began testing 3rd party cookie deprecation in Q1 2024, starting with a randomly selected 1% of all users (estimated to be 30 million individuals). They plan to continue increasing the number of users from June/July of this year.

At the time this document was written there has been no released results from Google on the 1% deprecation testing (initial timeframe is currently July 1st, 2024), leaving the true tangible impact of cookie deprecation on Chrome still relatively unknown. There is also no formal timeline from Google on the percentage phase out across H2 of 2024, leaving the current ecosystem relatively unaffected for the moment.

The original timeline provided by Google was to roll out a full deprecation by end of 2024. However, an announcement as of April 2024 have again delayed the deprecation timeline for the 3rd time since its original announcement in January 2020.

The delay is being driven by Google's need to provide more clarity to the UK's Information Commissioner's Office (ICO) and the Competition and Markets Authority (CMA), on how they plan to remove 3rd party cookies without unfairly hindering competition. Considering the recent announcement and complexity of this task, Google have not yet provided a concrete replacement date, rather citing early 2025 at this stage.

Cookies have been good to us.

Despite steady growth from its beginnings in 1994, the digital advertising industry's exponential growth began in the early 2000s when search engines, programmatic ad buying, and social media platforms emerged.

Fuelled by the mantra of "right ad, right person, right time", addressable ad buying, based on consumer data points, has revolutionised media buying. According to the 2024 Magna Media Australia Landscapes report[1], in 2022 digital advertising held a substantial share of budgets, comprising 71%, compared to 43% in 2015. In 2023, "Australia's advertising revenues increased to AUD $26.7 billion, reflecting a growth rate of +4.9%". Growth was seen across digital media owners' revenue ($13.6 billion), social media advertising ($6.3 billion), search advertising revenue ($9.9 billion) and digital video advertising increased by +9.3% to $2.3 billion.

Much of online advertising makes use of the basic and widely available 3rd party cookie, which have become part of the standard architecture of the web. They help with things like measuring the effectiveness of ad campaigns or enabling advertisers to reach valuable consumers. Below is a breakdown on the benefits advertisers, publishers and consumers have experienced due to 3rd party cookie use.

Stakeholder:	Benefits:	Example:
Advertisers	Addressable digital ad buying has reduced cost measures (CPMs, CPCs and CPAs) and improved outcome measures (conversion rates, ROI, completion rates and CTRs).	20% of consumers exposed to display advertising conduct related searches for advertised brands. 70% of website visitors retargeted with display ads are more likely to convert on your website.
Publishers	Despite some reluctance towards addressable digital selling, publishers discovered they could charge more for their inventory if they added consumer data which allowed audience targeting.	The Network Advertising Initiative (NAI) in 2009 found "behaviourally-targeted advertising" secured an average of 2.68 times as much revenue per ad as nontargeted. A 2015 BCG study found that "high-value targeting is…generally sold at premium rates" and for one publisher "inventory targeting its highest value audience segments achieves CPMs up to six times those for direct sales".
Consumers	An unspoken rule of the internet is that consumer can access an	Research has found that 71% of consumer prefer to see personalised

[1] MAGNA Atlas (magnaglobal.com)

	endless amount of free content and in exchange they receive targeted advertising. This is what CEO of The Trade Desk, Jeff Green, calls the quid-pro-pro of the internet.	advertisements, they are more likely to make a purchase when shown personalised ad and they are frustrated by impersonal shopping experiences.

Since the introduction of 3rd party cookie technology, there have been enormous benefits to all stakeholders in the market.

1. 3rd party cookies are the base technology used to deliver critical digital campaign tactics such as: re-marketing, sequential messaging, frequency capping etc.

2. Cookies have been one of the primary and most scalable methods for consumer data collection, creating a vast supply of data aggregators (organisations that collect large amounts of data) and segments (specific sets of data around core themes) to choose from when looking to implement data-driven targeting for campaigns.

3. Publishers have been able to lean on 3rd party cookies to generate targeted advertising revenue without the need to invest revenue, time and resource into building their own 1st party data collection. Importantly, until recent times, there was no requirement for a consumer to opt in to 3rd party cookies.

4. Mass attribution models were broadly possible thanks to the cookie's ability for cross-site tracking.

Change will be impactful and widespread.

While 3rd party cookies have supported some of the most fundamental campaign strategies and targeting that we have become reliant on, as we discussed above there is a recognised need to pivot in face of an advertising ecosystem that respects consumer privacy.

While the impacts of 3rd party cookie deprecation are still largely unknown and unqualified, there are certain strategies that we can be confident will require a pivot and others that are largely unaffected.

3rd Party Cookie Deprecation Impact:

Tactic	Impact	Impact Description	Alternatives
Frequency Capping	High	Frequency capping (the act of minimising showing too few or	Industry Solutions are still being tested and developed; however

		too many ads to a single consumer in a set time-period) today is largely dependent on 3rd party cookies. Therefore, the ability to cap frequency across inventory and strategies will be impacted.	current alternatives are to use frequency capping within each publisher's environment together with persistent ID solutions (such as login data) in buying platforms.
Sequential Targeting	High	Sequential targeting is the ability to show ads in a sequence, over time, to a consumer. The ability to capture which audiences have been served an impression to then send a follow up creative will be heavily compromised by the deprecation of 3rd party cookies.	The solution will be a combination of replacement solutions within each walled garden/platform and will involve building a modelled solution based on what can be collected from 1st Party Data (1PD).
Audience Targeting	Medium	Providers who have historically created segments built from 3rd party cookies will be impacted.	Solutions such as Google's Privacy Sandbox and data providers such as Acxiom (who have already begun creating data stacks built from anonymised personally identifiable information, or PII)
Look-a-like Modelling	Medium	Look-alike modelling which has previously been performed against an aggregated cookie-based data set will be impacted by deprecation.	Solutions such as Google's Privacy Sandbox will allow for AI generated modelling on 1st party data, and data providers and media buying platforms (like Facebook) will model against consented PII data instead of cookies.
Onsite consumer experience	Medium	Unbeknownst to many, 3rd party cookie deprecation can also impact website page functionality and experience. Some critical consumer journey experiences are built on 3rd party cookies such as shopping cart to payment flows for non-logged in consumer, publisher sign ups and the ability for onsite preferences to be saved.	A site audit is necessary to ensure that no critical consumer journey or site functionality is currently operating with the use of 3rd party cookies. If this is found to be the case, pivoting quickly to rectify these workflows will be critical.

Measurement	High	Brands have often been dependent on digital signals to understand the impact of media on business outcomes. Ad servers, being one of the more widely adopted solutions to date, are heavily cookie-based - meaning that their impact assessment value will likely diminish as cookie information decreases. Alternative solutions in the market are in development and brands should begin testing to understand what specifically works for them.	Each media buying platform is working to mitigate these impacts. Trade Desk alternatives are discussed later, and Google have their reporting API and ADH clean room as solutions to fill the gap deprecation presents, although these require set up and management. The value of Media Mix Models is also becoming increasingly important. Brands are increasingly investing in this cookie-less space to better understand the holistic impact that media has on business performance.

Cookies aren't the only change; privacy is shaking things up.

While privacy is a hot topic in Australia given the impending legislation review, it is not new news around the globe.

The General Data Protection Regulation (GDPR, put into effect on May 25th, 2018) is a data privacy and security law that was drafted and passed by the European Union (EU). It imposes obligations onto organisations anywhere, so long as they target or collect data related to people in the EU.

Additionally, the California Consumer Privacy Act (CCPA, which came into effect on the 1st of January 2020), introduced a range of new rights, obligations, and enforcement measures to facilitate greater protection of consumers personal information. Following California's lead, four other states — Colorado, Connecticut, Utah, and Virginia – are enforcing new GDPR-inspired statutes throughout 2023.

On the 26 of October 2022, the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 was tabled in Parliament by Australia's Attorney-General, Mark Dreyfus and was quickly legislated. This was done in response to the Medibank and Optus data breaches. The Bill aimed to immediately provide The Office of the Australian Information Commissioner (OAIC) enhanced powers to request information and conduct assessments, introduce information sharing powers and significantly increase penalties for serious or repeated privacy breaches. It is a key point to understand that OAIC already

has significant enforcement powers and fines for serious breaches have already been increased for both company and its directors. To speak plainly, these penalties have been increased to the point that a fine that may have previously been considered 'palatable' as a risk/cost to a business is now today large enough to significantly impact a businesses ability to continue functioning.

Secondary to OAIC enforcement, the Bill also proposed amendments to the Privacy Act (of 1988), which is expected to be subject to further reform soon.

If legislated, these changes will alter the way the industry currently views personal data and therefore will likely change the way consent is derived, how that data might be accessed, and the controls placed on both the data supplier, controller, and processor in the handling of this data.

Of the 116 proposals in the Privacy Act Review Report, the Government agreed to 38 proposals, agreed in-principle to 68 proposals and noted 10 proposals. 'Agrees in-principle' indicates that further engagement with entities and a comprehensive impact analysis is needed before a final decision on implementation.

The Attorney-General's Department will lead the next stage of work, which will likely involve legislating the first 38 agreed amendments. The sentiment in the advertising industry in early 2024 was that the Government would prioritise the first 38 agreed amendments into legislation towards the end of the year. With the announcement of reform being tabled in Parliament in August we can be confident the Government is prioritising this reform; however, it remains to be seen what topics they will focus on, and whether this will still be looked at in two waves.

Another important thing for readers to note is that the Government has made it clear that while they will learn from overseas examples, such as GDPR and CCPA the reform will be unique to Australia. The main take away from this should be for businesses not to be compliant that they are compliant with overseas laws, they will need to follow local reform specifically.

Below is a topline summary of some key take outs for the Agreed 38 Principles:

Status From Government:	Decisions:	What does this mean?
Declined	AG has elected not to extend protection to de-identified data.	De-identified data will not be subject to the same level of protection as personal information. This could make it easier for organisations to collect and use de-identified data without the consent of individuals.
Declined	Political entities included in reform.	Political entities will not be subject to the same privacy laws as other organisations.

Declined	Consumers will not have an unqualified right to opt out of targeted advertising.	Consumers will not have the right to opt out of targeted advertising in all cases. Organisations may still be able to use personal information to target advertising if they have a legitimate interest in doing so.
Agreed 38, first wave	Added protection from facial recognition and new tech.	Organisations will need to take steps to protect individuals from the risks associated with facial recognition and other new technologies. This could include obtaining consent from individuals before collecting and using their biometric data.
Agreed 38, first wave	Automated / AI decision making transparency.	Organisations will need to be transparent about how they use automated decision-making systems. This could include providing individuals with information about how these systems work and how they affect their personal information.
Agreed 38, first wave	Enhanced security requirements.	Organisations will need to implement enhanced security measures to protect personal information from unauthorised access, use, or disclosure. This could include measures such as encryption, access controls, and security audits
Agreed 38, first wave	Protection of Children & Vulnerable	Organisations will need to take steps to protect the personal information of children and vulnerable individuals. This could include measures such as obtaining parental consent before collecting and using the personal information of children.
Agreed 38, first wave	IC Power & Enforcement	The Information Commissioner will have increased powers to enforce the privacy laws. This could include the ability to issue fines and penalties for violations of the privacy laws.

Agreed 38, first wave	Overseas data flow will need to prescribe to APP (Australian Privacy Principle) policies	Organisations that transfer personal information overseas will need to ensure that the recipient of the data complies with the Australian Privacy Principles. This could include measures such as entering into data transfer agreements with the recipient of the data.

While a lot is still unclear, there are some primary amendment themes we do know about.

- The introduction of Enforcement & Governance – continued enforcement power for OAIC to govern and enforce privacy breaches. Recent announcements by the Privacy Commissioner Carly Kind have emphasised that OAIC's focus will be on proactive and proportionate work, *even before the Privacy Act reforms are introduced.*
- The introduction of legislation for child protection & protection of vulnerable individuals in the community.
- The introduction of a 'fair and reasonable' test for the collection, use and disclosure of personal information, serious invasions of privacy, the right for Australians to sue for privacy invasions and the emergence of AI technologies.
- New and enhanced rights for individuals, such as the right to erasure, the right to de-index internet search results and new requirements for businesses around retention periods for personal information they collect.

Importantly for the advertising industry, the Government has recognised that consumers do not have a right to unqualified opt out of advertising. This essentially means that consumers can't say no to targeted advertising or opt out completely. Peter Leonard, a data and technology business consultant and lawyer, at the 2024 Sydney Programmatic Summit made an interesting comment. He spoke to the point that *consent matters, but transparency disclosure really matters*, phrasing it more simply as the government are not so much concerned that you are doing it, they are more concerned with what you can do.

Below is a summary of some of the key industry views on what we know so far:

Change:	Industry View:
Decision to decline consumers unqualified right to opt out of targeted advertising.	The IAB and ADMA are positive towards the ruling to not allow unqualified opt out of targeted advertising.
Broadening of PII definition	There is concern that the definition of PII data is too broad. The ACAP2023[2] survey provides more insight into how the public views Personal Information (PI) data.

[2] Australian Community Attitudes to Privacy Survey 2023 | OAIC

A testing framework for what is considered Fair & Reasonable when collecting and using consumer data.	The industry has expressed concern about the currently vague definition of what is 'fair & reasonable' with regards to use of PI data. There are discussions that what is considered to be a fair and reasonable reason for collecting and using consumer PI information could become vertical or organisational based, for example Healthcare could be treated differently to advertising
Consent Management.	There is more responsibility for entities to be accountable and less pressure on the public to understand privacy. But consent fatigue is still a factor that is unresolved.
Small businesses won't be exempt.	Small business will not be exempt as previously thought. However, there is a concern over cost to small businesses to manage provisions.
Politicians will get an exception from the Act.	They will still have to follow the guidelines, but it will be more lenient. The same goes for research companies.
Added Government certifications are coming for businesses.	There will be requirements for businesses who are collecting consumer PI data to acquire Australian Privacy Principle (APP) certifications and conduct Data Audits.

Something for readers to keep their eyes out for is the Australian Competition & Consumer Commission (ACCC) March 2024 Interim Report where the ACCC will consider potential competition and consumer issues in the supply of data broker services in Australia (3rd party data services). The report will focus on data brokers, how they collect information about consumers from various third-party sources and how they share it with organisations. The report is the eight interim report of the Digital Platform Service Enquiry which launched in 2020. After submissions from the industry were invited, the ACCC was due to provide the report in March of 2024, however this timeline has been delayed with an unclear new deadline. This will be an important outcome with the Government labelling it a 'weak spot' due to recent data breaches involving 3rd party data providers that have shone a light on the need for organisations to ensure their privacy obligations are passed onto these data suppliers. This is an important development for the industry as many organisations use 3rd party data providers to target their 'unknown' consumers and identity spines that fuel persistent ID solutions are often built in partnership with 3rd party data brokers. Limitations or sever impacts to the ability for 3rd party data brokers to operate in this market would have wide reaching impacts on the ad industry.

As one door closes, a few are set to open.

As discussed above, both privacy changes and 3rd party cookie deprecation are going to have impact on the industry in a variety of ways and that impact is not largely known at this stage. The good news is that we have already begun to see the emergence of

solutions that will allow the industry to move forward while still respecting consumer privacy.

However, with the emergence of such a wide variety of solutions comes cost implications and fragmentation, which will cause disruption and challenges for all parts of the advertising ecosystem. These solutions need to be carefully navigated and tested in the context of each specific advertiser and their media activity.

Solution	What to learn	Current state
Persistent ID Solutions	A persistent ID solution in the advertising industry is a method of identifying a consumer across multiple devices and platforms, usually using data from logins. This allows advertisers to track behaviour and preferences over time, and to deliver targeted advertising. Importantly these persistent IDs are built from consented, anonymised, and encrypted PII data (such as an email address).	Examples of some solutions in market are the Universal ID (UID2.0), which is open to industry (but while championed by The Trade Desk it currently doesn't have an organisation willing to administrate the data), and LiveRamp's Authenticated Traffic Solution (RAMPID). While these solutions are currently experiencing scalability challenges, they are uniquely placed to thrive once publisher adoption increases.
Google Privacy Sandbox	Privacy Sandbox is a set of proposals from Google Chrome to improve consumer privacy while still allowing advertisers to target their ads effectively through media buying platforms.	The fundamental shift here is that instead of buying platforms (such as DV360) being able to use a list of users browsing behaviour created through the collection of data via 3rd party cookies, a user's data will instead remain on-device (within their browser) and will be anonymised and aggregated and then sent to buying platforms via APIs. Privacy Sandbox includes different technologies such as Topics API, Protected Audiences API and Attribution Reporting API.
AI Product Extensions	Specific products that will allow client 1st party data to be fed through generated models to aggregate and extend the potential of 1st party data.	Providers like Google are championing this space with products such as Value Based Bidding and PMAX as well as a

		step towards leveraging 1st party data. Some other examples of these are Enhanced Conversions API, Customer Match, ADH and PAIR available in DV360 and/or Google Ads.
1st party data collection and use for Brands.	The collection of consumer Personal Information for marketing purposes in exchange for free or paid content as well as a better onsite experience (personalised logged in experience). This tactic isn't new, but under current circumstances is now more crucial than ever for brands. Not only from a compliance and scale perspective, but also for consumer value.	Crucial for brands for personalisation, re-engaging consumers, and cross selling. Investment in CDP technology for data collaboration, storage & analysis and clean room technology (such as LiveRamp) for data distribution and collaboration will assist here.
1st party data collection and use for Publishers.	1st party data collection and use is a strategy that some publishers like Broadcast Video on Demand (BVOD) publishers (such as Seven West Media, Nine, SBS and Paramount) have been actively investing in for a number of years to future proof their business.	Publishers who have been collecting 1st party data have already begun to utilise it in the form of Seller Defined Audiences (SDAs). This involves using their 1st party data to create segments which are then sold across their inventory.
Contextually based targeting	Allows for the targeting of valuable consumers based on the content they are consuming rather than cookie information stored on their browser.	Contextual targeting will see a huge re-emergence in 2024. This will come in the form of contextual content from publishers as well as from technology partners who use the Google Sandbox TOPICS API to build their own contextual solutions.

How do brands move forward from here?

On the privacy front, investing in the hiring of a Data Privacy Officer is a first step for brands. This role is critical in ensuring that a brand is taking the appropriate steps to ensure they are prepared for legislative changes. Given the OAIC has already been

provided greater enforcement powers and significant financial fines for data privacy breaches are already in play, it is imperative that brands have their house in order. If not done already, brands should consider investing in technology solutions that centralise their data and create a single customer view as well as data hygiene tactics for their CRM. One area that Data Privacy Officers should be looking into is Privacy Enhancing Technologies[3], referred to as PETS. PETS are digital solutions that allow for information to be collected, processed, analysed, and shared while protecting data confidentiality and privacy. The main three PET types are:

- Data Obfuscation Tools, which add 'noise' to datasets by removing identifying details to enable machine learning and information verification to be done in a privacy compliant manner.
- Encrypted Data Processing Tools, which allow data to remain encrypted while in use, therefore avoiding the need to decrypt the data when being used.
- Federated and Distributed Analytics, which allows analytic data queries to be run on data that is not accessible to those executing the task, therefore safeguarding the data further.

PETS in AdTech can be utilised across data collection, technology ecosystems (such as data platforms, AdTech platforms and devices) and data activation. These tools should be looked at internally for brands to ensure that their internal ecosystems are securely set up for the collection and use of data in relation to the Australian Privacy Legislative changes.

Brands should also be cognizant of the fact that the Australian Privacy Commissioner, Carly Kind, is looking to ensure that not only cookies are reviewed from a privacy perspective, but pixels and tags as well, to ensure that the industry is not just replacing the cookie with hidden tags that do more harm than good. As we march towards cookie deprecation, brands should be ensuring that their Privacy Officer and teams are invited on the full 1st party journey, including the use of tags and pixels.

Once you have a data ecosystem that is compliant in how it collects, stores and transfers data, as well as manages opt-outs, the next step is to begin investing in the collection of 1st party data. This, however, should be done with an appropriate strategy in place to ensure that the data that is collected is accurate, useful, and fit for purpose. Tactics such as collecting data through competitions and prizes may be quick and bountiful, but brands should question whether they provide accurate information, and the extent to which consumers are allowing you to keep that data for long term engagement (instead of immediately opting out post competition). Brands should be focusing on the value exchange for consumers to encourage data collection with longevity and a continued relationship in mind, this could be through loyalty programs or sponsorship/brand collaborations.

[3] https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf121be4-en.htm

On the 3rd party cookie front, as we have discussed through this paper, significant change is coming over the course of this year, and while disruption should be expected there are steps brands can be taking to get prepared. As we move to a world no longer grounded in 3rd party cookies but instead to an environment where advertisements can only be targeted to a consumer if they are authenticated (logged into a site) brands will need to either collect their own consumer PII as discussed above, or they will need to either invest in direct partnerships with publishers who are collecting PII, or work with identity partners who have integrations into a range of publisher sites (such as Infosum, Liveramp, Acxiom and others). Alongside integrations to internal mart-tech such as customer data platforms (CDPs), media activation platforms like demand side platforms (DSPs) and social media channels, brands should also consider looking to explore and invest in the licensing of 2nd and 3rd party data via identity partners. These integrations will allow brands to match their 1st party data to the identity partners offline collected data which can then be used for audience insights, audience builds, modelling, media activation, and measurement using identity-based IDs. Importantly, this will help brands to reach their 'unknown' customers (those who are not their customers already).

It is worth noting that when looking to assess identity solutions, interoperability is key. As we discussed above technology in this space can come with a hefty price tag, so ensuring your identity partner can integrate seamlessly with your internal data ecosystems and provides access to a variety of publisher inventory and media buying technology should be a priority.

Conclusion:

As this paper has explored, significate changes are coming in the form of 3rd party cookie deprecation in Chrome and impending changes to the Australian Privacy Act.

While these changes are certainly for the better, and critical to ensuring that consumer privacy is treated respectfully, it is presenting challenges to publishers, agencies, and brands due to how imbedded 3rd party cookies have become in the digital advertising ecosystem.

Considering 3rd party cookies have been used in digital advertising for so long it should not be surprising that they are so embedded in many of the tactics and strategies we have come to rely on such as frequency capping, data collection, personalised advertising, onsite experience, and remarketing - alongside many more. Given the proliferation of 3rd party cookies means that their deprecation will mean changes will be impactful and widespread to all stakeholders.

Cookie deprecation is not the only change the industry is facing. Driven largely by consumer demand, Privacy Legislation changes are set to shake things up. Australia is following the EU and certain States in American in reviewing the Privacy Act to ensure greater protection of consumers personal information.

Of the 116 proposals in the Privacy Act Review Report, the Government has agreed to 38 proposals, agreed in-principle to 68 proposals and noted 10 proposals. The reform is officially set to be tabled in Parliament in August 2024, and while there is still uncertainty about what topics and proposals the Government will focus on and how they will roll it out, this should garner the attention of all Privacy Officers and legal teams so that they are ready for anything.

It's not all doom and gloom though, as one door closes a few are set to open. Over the last couple of years, in preparation for these changes, we have seen the rise of new privacy safe solutions such as Sandbox Solutions, Privacy Enhancing Technologies and Persistent ID technology to recap a few. There will also be a re-emergence of tactics the industry has largely stopped using such as Contextual Targeting and the renewed focus on 1st party data usage. The key for marketers and agencies will be in evaluating those solutions and creating the best mix for each brand, as no solution in this space will be a one size fits all.

For media agencies, the need to assess your client's media activity to determine their cookie dependency through the lens of tactics, strategies and platforms being used is an important first step. These audits will ensure you have time to transition your media buying to ensure minimal impact for your campaigns. Also important is the upskilling of programmatic traders and staff with any new features from DSPs regarding tactics, optimisation features, reporting and implementation needs.

Importantly for brands, there are steps that can be taken to be ready for the changes such as investing in a Data Privacy Officer to ensure internal ecosystems are set up to be compliant in the new privacy world, as well as investing in technology and partnerships that allow for the efficient and safe use of data. Equally, while 1st party data collection is key, ensure you have a strategy for what you are collecting so that the data is valuable and fit for purpose.

The recent announcements about the further delay to Chrome’s deprecation of cookies shouldn’t be seen as a reason to pause. These changes will occur, and as this paper has mentioned have already occurred on other browsers. While the delay may give the industry (agencies and brands) more time to get their ducks in a row, it should not be seen as a reason to slow down on future proofing your business and media against inevitable changes.

Amidst a landscape of shifting digital privacy norms and technology, Kinesso remains committed to not just navigating these changes in partnership with the wider ecosystem but also ensuring our clients are fully informed and prepared. This includes transparency about how these changes impact media dollars and reporting, a crucial aspect often glossed over in industry discussions.