AUSTRALIAN DIGITAL ADVERTISING PRACTICES

2020 UPDATE

AANA

iab. australia

mfa media federation of australia

CONTENTS

INTRODUCTION

The Australian Digital Advertising Practices have been created specifically for advertisers by a cross-industry team of advertisers, agencies, digital publishers, ad tech vendors and subject matter experts.

Endorsed by the Australian Association of National Advertisers (AANA), Interactive Advertising Bureau (IAB Australia) and the Media Federation of Australia (MFA), the Practices seek to:

- Educate: providing a common understanding of the digital advertising ecosystem (and dispel common misunderstandings)
- Encourage shared responsibility: ensuring advertisers, agencies, publishers and digital platforms have shared insights and responsibilities for digital spends and outcomes
- Enable trust and confidence: building confidence and trust in digital advertising

While the Australian Digital Advertising Practices have primarily been developed for advertisers, given the rapid pace of change within the digital advertising market we strongly encourage all players within the digital ecosystem to familiarise themselves with the content to better inform conversations with current and future clients and partners.

These Practices build upon the first version published in July 2018 and now include technical, market and regulatory updates, as well as an expanded section on the important subject of consumer privacy.

There will be future updates to Australian Digital Advertising Practices to align them with significant changes in the market. Since their original publication in 2018 we have seen a number of studies and reviews around the world looking at these topics. The working group for this document will also review any findings and recommendations which may come from the ACCC Digital Ad Tech Inquiry which is scheduled to make its interim report in December 2020 and final report in August 2021.

PRINCIPLES

The following operating principles guide the approach we have taken and the content of the Australian Digital Advertising Practices. They are:

1. CHAMPION THE CONSUMER EXPERIENCE
A better user experience will lift key quality metrics and overall campaign effectiveness.

2. EDUCATE TO INSPIRE CHANGE
Through best practice education, communication and a clear understanding of metrics, we seek to inspire change. We cannot force or mandate it.

3. SHARED OWNERSHIP AND RESPONSIBILITY
All participants in the value chain need to take responsibility for their own knowledge and understanding. Shared ownership and responsibility are imperative.

4. EVERY VALUE CHAIN IS UNIQUE
Each advertiser's needs are different. The approach to improving the value chain needs to be optimised for each advertiser's needs and partner arrangements. The advertiser must be accountable for their individual value chain.

5. FAIR VALUE FOR OUTCOMES DELIVERED.
Value is created through quality and price, therefore, adopting best practices to deliver better outcomes may cost more.

WHAT ARE THE AUSTRALIAN DIGITAL ADVERTISING PRACTICES?

The Australian Digital Advertising Practices are a starting point for advertisers, agencies, ad tech vendors and digital publishers to resolve how they will operate together. They do not solve all issues but they are an important first step in building trust and instilling confidence in the digital advertising value chain.

Designed to be read and understood in an hour or less, the Practices address six digital advertising value chain issues which represent the highest areas of concern and the greatest lack of understanding within the industry. Each of these issues are addressed in modules, with ad fraud and brand safety combined into one module, because while these two issues are separate and significantly important, the practices and tools employed to address them are often similar. To avoid duplication, the recommended practices for these concerns have been combined, however, this does not diminish the importance of either.

1. **DIGITAL VALUE CHAIN**
2. **VIEWABILITY**
3. **AD FRAUD AND BRAND SAFETY**
4. **DATA GOVERNANCE**
5. **CONSUMER PRIVACY**

Each module includes a checklist of questions and areas to consider so that informed decisions can be made. The modules also include links to specialist resources to provide access to deeper knowledge and further detail.

WHAT THE AUSTRALIAN DIGITAL ADVERTISING PRACTICES ARE:

- Designed to inform and educate participants to ask the right questions and make informed decisions.
- Putting accountability for the solution into the hands of the participants.
- Practical and for everyday use through a checklist approach.
- Flexible to fit individual advertiser or partner needs.
- Available to all.
- Designed for Australia and the way we work.

WHAT THE AUSTRALIAN DIGITAL ADVERTISING PRACTICES ARE NOT:

- Fixed standards or targets.
- Mandated solutions.
- The same answer for every advertiser or partner.
- International answers trying to address local issues.

WHAT DOES SUCCESS LOOK LIKE?

The common goal for all five modules is to create a consistent and educated understanding that enables all parties to make informed decisions.

1. **A HIGH LEVEL OF ADOPTION ACROSS THE DIGITAL ECOSYSTEM**
2. **CONTINUOUS IMPROVEMENT OF BEST PRACTICES**
3. **FAIR VALUE FOR ELEVATED SURETY**
4. **ELEVATED TRUST AND CONFIDENCE IN HOW AND WHERE TO INVEST IN THE DIGITAL ECOSYSTEM**
5. **ESTABLISHING A COMMON LANGUAGE ACROSS THE VALUE CHAIN**
6. **ELEVATED ADVERTISER CONTROL AND ACCOUNTABILITY AS A RESULT OF MAKING INFORMED DECISIONS**
7. **A SET OF CLEAR AND PRACTICAL USABLE SOLUTIONS**
8. **KEY STAKEHOLDERS ASKING SMART QUESTIONS**

We will measure success on a regular and quantitative basis against the overall KPI of building trust and instilling confidence in the digital advertising value chain for all participants and optimising its value to the wider industry. Tracking of progress and performance against this will help inform further reviews and continuous improvement of the best practices.

DIGITAL VALUE CHAIN

THE CHALLENGE

The digital advertising industry has evolved to become a complex ecosystem of interconnected technologies and services. While this enables a variety of advertising outcomes, it means the industry is awash with terms that many do not fully understand.

As a result, it is difficult for advertisers to understand the benefits of each individual technology, data or service, how these technologies might work together and, how to get the best value from their digital investments.

This confusion can impact confidence and trust in the digital value chain. To counteract this we must:

- Provide clear and simple information about the various possible supply chain elements and describe their benefits.
- Demonstrate which supply chain elements are fundamental building blocks (essential to executing a buy) and which are optional.
- Build an understanding of the mix of media to truly drive business outcomes.

THE DIFFERENT DIGITAL ADVERTISING TRADING MODELS

There are a variety of digital advertising models:

- Advertiser in-house
- Independent trading desks
- Agency trading desks
- Bespoke hybrid models

The buying process for digital display advertising can be complex and does necessitate layers of data and technology to assist in making informed decisions. There are a variety of digital advertising models available to advertisers: advertiser in-house, media or digital agency services, independent trading desks, and bespoke hybrid models. It is important for advertisers to understand the pros and cons of these models, interrogate them based on business requirements and be accountable for the type of model ultimately chosen. This must form part of an advertiser's contractual terms with all media partners.

AGENCY TRADING MODELS

Agency digital advertising services and the way they are delivered along with the remuneration arrangements between agencies and clients have evolved over the years based on client requirements. There are two key models which agencies operate with their clients, the guaranteed outcome-based model and the itemised model, these can sometimes also be referenced as undisclosed and disclosed. Both models have merits for advertisers and depend on an advertiser's requirements and preferences.

Guaranteed Outcome based model: The outcome-based model was the most common model implemented when agencies provided programmatic services to advertisers initially. In this model, the agency will guarantee an outcome, such as a CPM (Cost per Thousand) to reach a specific audience or a Cost per Click (CPC) Cost per Acquisition (CPA). On this basis, the agency guarantees a price to the advertiser at the time a media plan is approved, before any bidding has taken place.

- The CPM quoted to the client is inclusive of all costs, including the media publishers' fees, third party platform fees and any data costs.
- There is a set price (CPM) guarantee for an advertiser to reach an audience and an agreed outcome
- The advertiser has less involvement and decision making in the process, which could be seen as a positive or negative by an advertiser depending on their own resources.

DIGITAL VALUE CHAIN

Itemised Model: The itemised model is the most common model in today's marketplace. Over time, as advertisers invested more in programmatic campaigns, they have sought more visibility over the cost components, in part to ensure they are receiving value for this increased expenditure. As a result:

- This model itemises all costs and fees to be implemented in a campaign in a media plan, so that an advertiser can see and approve the quantity of media, third party data costs and the third-party platform fees used to deliver an audience.
- The agency is remunerated through a service fee which is most often a percentage of the total approved campaign costs, that is an agreed percentage of all costs including media and third-party costs such as data costs and platform fees.
- The agency may alternatively be remunerated by an FTE (Full Time Equivalent) based model where the agency charges a fixed retainer based upon the number of staff required to service the client, that is the direct salary costs of those staff, an overhead recovery and agreed profit margin on those direct salary costs and overhead.
- An advertiser approves the cost components on the media plan and pay those costs regardless of outcome.
- The advertiser takes a more active role in agreeing the media, data sources used as well as the platform.

Under either model that an agency may agree to implement with an advertiser, it is always clearly defined in the advertiser/agency contractual agreement as to what visibility it is agreed the advertiser has in regard to the programmatic supply chain. This principle is reinforced in the MFA Transparency Framework signed onto by all MFA members.

DIGITAL VALUE CHAIN CHECKLIST

This checklist has been prepared to provide a framework for discussion between advertisers, agencies, ad tech providers and publishers around the technology, data and services most appropriate for a range of different buying circumstances or outcomes.

1. Understand the technology that is currently in place

Begin by understanding what (if any) digital media capabilities are already place.

Work with your agency, technology and publishing partners to establish a detailed explanation of each component in the digital value chain. Identify the services as well as the costs and value they provide. Refer to the tables on pages 8 and 9 to check if these are optional requirements.

This knowledge will provide a useful platform to inform discussion on what (if any) changes may be required.

2. Identify how each component of your digital set-up is adding value

Explore how each component in your current set-up is contributing to the delivery of your objectives. Technology, data and services all come with costs attached – is this investment creating incremental value?

For each dollar invested, identify and understand the base cost of the media (e.g. what goes to the publisher) from the optional or additional services you may have purchased such as a data-management platform (DMP) or an ad verification service. This will ensure you can make an informed judgement on the overall value.

DIGITAL VALUE CHAIN

3. Examine and decide on media buying objectives

Ensure you are clear on your media buying objectives before briefing media partners so they can design a suitable approach. For example, are you trying to drive awareness of a brand or product, push people to a website or sell a product online?

Being clear about what you want to achieve will help partners to design an approach that is suitable.

4. Programmatic or direct?

There are two main ways to buy digital media – programmatic or direct.

Programmatic buying involves the use of automated buying and selling technologies, matching advertiser and publisher in real-time.

Direct buying follows a more traditional process where the buyer and seller conduct a negotiation followed by the placement of an insertion order.

The best buying method will be determined by your campaign objectives. A combination of the two may be required.

5. The essential elements

Ensure you understand the base-line technology requirements for each type of media buy such as whether certain technology is essential to execute specific types of digital media buys. For example, it is not possible to execute a programmatic buy without a demand-side platform (DSP).

Refer to the tables on pages 8 and 9 to determine the technology that will be essential.

6. Decide what technology will add value

Beyond the essential technology, additional technology can be deployed to drive more evolved buying outcomes such as enhanced brand safety, viewability, and audience targeting.

You need to understand the trade-offs that may be required if you push for one outcome over another. For example, pushing hard for high levels of viewability may compromise the ability to drive cost-effective reach.

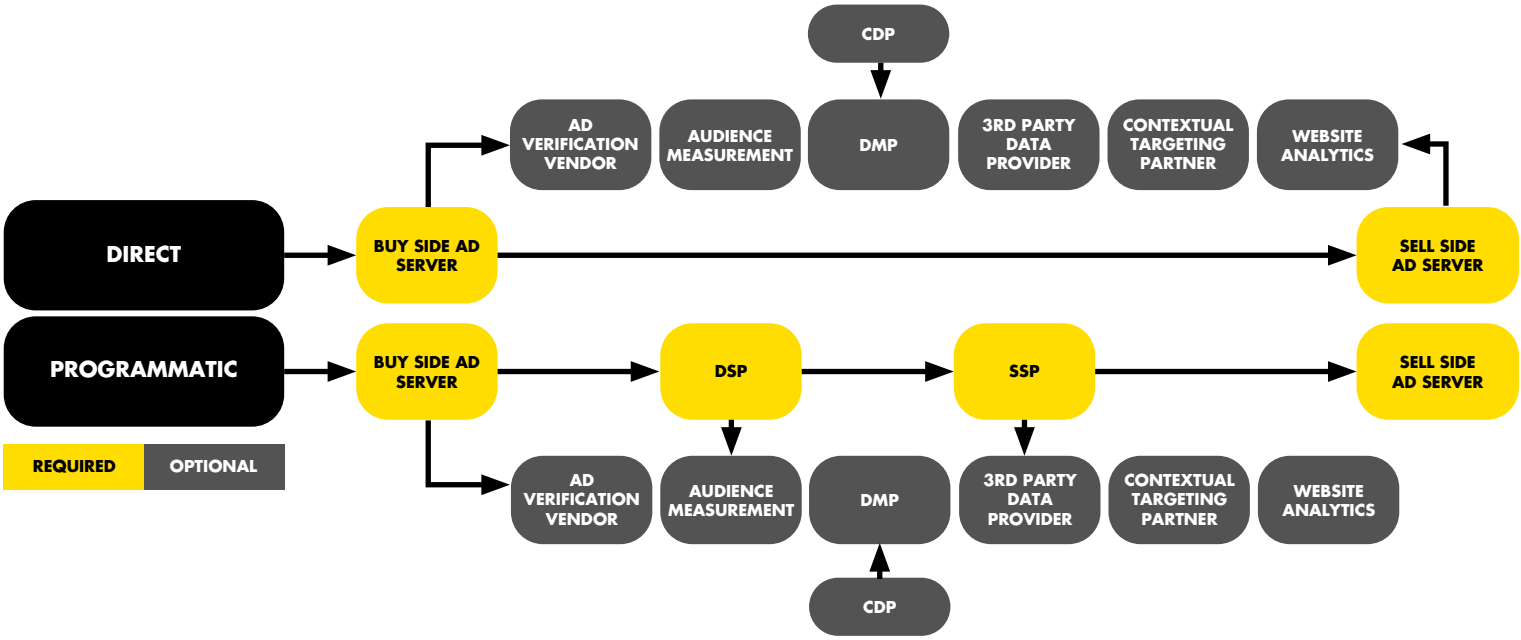
Everything is a balance. What is the right balance for you?

7. Choose metrics to track outcomes

To understand the difference between the media that is driving the desired outcome and the media that is not, you need to establish a clear set of metrics that cover both. You should begin by ensuring you understand the base-line technology requirements for each type of media buy - branding performance and direct response.

DIGITAL VALUE CHAIN

KEY TECHNOLOGY AND DATA SERVICES: DIRECT AND PROGRAMMATIC



DIGITAL ECOSYSTEM ELEMENT	SIMPLE DESCRIPTION	EXAMPLES
Buy-Side Ad Server (Third-party Ad Server)	A web-based platform for buyers to host, manage and serve digital assets for advertising campaigns. Its primary goal is to centralise and standardise delivery and performance data with a uniform methodology for counting across key metrics. Some may also be able provide viewability capabilities (e.g. Google TrueView).	Google Marketing Platform, Adform, Flashtalking, Sizmek by Amazon
Audience Measurement	Best defined as the independent measurement of digital advertising audience delivery across all device types. Audience measurement can refer to the measurement of ads and content/media environments.	Nielsen, Comscore, GfK, Roy Morgan
DMP	A Data Management Platform (DMP) is used to collect, store and manage online and offline data sets to gain insights before creating actionable segments to target digital campaigns.	Salesforce DMP, Lotame, Neustar OneID, Adobe Audience Manager, Eyeota, Oracle BlueKai
CDP	A Customer Data Platform (CDP) is a technology capable of collecting data from multiple online and offline interactions and matching them to a single customer profile. One main feature is they can profile interactions from anonymous customers and retroactively tie that data to a customer once it is identified.	Lexer, Tealium, Salesforce, Oracle CX Unity
DSP	A Demand-Side Platform (DSP) handles automated media buying across multiple inventory sources using targeting, data and real-time optimisation. The DSP is designed to buy an audience versus an objective. Its goals are to pay the lowest possible price for inventory whilst fulfilling the buyer's campaign objectives. A buyer will use a DSP to access publisher inventory made available via an SSP.	Google Marketing Platform (DV360), The Trade Desk, MediaMath, DataXu, Amobee, Adobe Advertising Cloud, Xandr Invest, Verizon Media DSP, Quantcast, Amazon
SSP	A Sell-Side Platform (SSP) is used by sellers (publishers) to make digital inventory available for DSPs to bid upon. The SSP looks to maximise yields for the seller whilst meeting the buyer's key campaign objectives.	Google Ad Manager (Ad Exchange), Rubicon Project, Xandr Monetize, Telaria, PubMatic, Verizon Media Exchange, Index Exchange, OpenX
Sell-Side Ad Server (Publisher Ad Server)	A Sell-Side Ad Server is a web-based platform for publishers to store, manage and serve digital assets across digital properties. Its primary functions are to manage the pacing and delivery of advertising campaigns and provide data on campaign performance. Some platforms may specialise specifically in mobile, in-app environments or video.	Google Ad Manager, Xandr Monetize, SAS Intelligent Advertising, Adnuntius, SpotX, Smart AdServer
Ad Verification Vendors	Ad Verification Vendors offer technology that can give independent data on measurement metrics including viewability, fraud and brand safety.	IAS, Oracle Data Cloud, DoubleVerify
Third-Party Data Providers	Third-Party Data Providers are agents that build audience data sets through partnerships and integrations with external audience collection providers. This data can then be used to target audiences via a DSP or DMP.	Eyeota, Audience360, Lotame, Equifax, Oracle Data Cloud, Quantium
Contextual Targeting Partners	Contextual Targeting Partners offer technology that determines the content of a web page allowing programmatic buyers to deliver contextually targeted ads.	Oracle Data Cloud, Peer39, 4D
Website Analytics Platforms	Website Analytics Platforms are platforms that track and report on online traffic. These platforms can optimise digital properties and analyse online user behaviour. While they are optional, they are essential to understanding website visitor behaviour.	Google Marketing Platform (Google Analytics), Adobe Analytics, Quantcast

DIGITAL VALUE CHAIN

BUYING OUTCOMES

This table shows the same list of technologies and highlights whether each element plays a role in contributing to a range of additional buying outcomes.

(Y= yes, N= no, P= possibly).

	Buy-Side Ad Server	Audience Measurement	DMP	DSP	SSP	Sell-Side Ad Server	Ad Verification Vendors	Third-Party Data Providers	Contextual Targeting Partners	Website Analytics Platforms
Creative Hosting	Y	N	N	P	N	Y	N	N	N	N
Creative Optimisation	Y	N	N	N	N	Y	N	N	N	N
Campaign Reporting	Y	Y	N	P	N	Y	Y	N	N	N
Data Management	P	N	Y	N	N	P	N	N	N	Y
Audience Targeting Precision	N	Y	Y	Y	Y	P	N	Y	N	N
Ad Placement Precision	N	N	N	Y	Y	P	Y	N	Y	N
Brand Safety Measurement	N	N	N	N	N	N	Y	N	N	N
Viewability Measurement	N	N	N	N	N	N	Y	N	N	N
Attribution	Y	N	P	N	N	N	N	N	N	P
Examples	Google Marketing Platform, Adform, Flashtalking	Nielsen, Comscore, GfK, Roy Morgan	Salesforce DMP, Lotame, Neustar OneID, Adobe Audience Manager, Eyeota, Oracle BlueKai	DV360, The Trade Desk, MediaMath, DataXu, Amobee, Adobe Advertising Cloud, Xandr Invest, Verizon Media DSP, Quantcast, Amazon	PubMatic, Rubicon Project, Xandr Monetize, Telaria, Index Exchange, OpenX	Google Ad Manager, Xandr Monetize, SAS Intelligent Advertising, Adnuntius, SpotX, Smart AdServer	IAS, Oracle Data Cloud, DoubleVerify	Eyeota, Audience360, Lotame, Equifax, Oracle Data Cloud, Quantium	Oracle Data Cloud, Peer39, 4D	Google Analytics, Adobe Analytics, Quantcast

DIGITAL VALUE CHAIN

THE DIFFERENCES BETWEEN DMPs AND CDPs

DMPs will work primarily with anonymous behavioural data such as cookies, device IDs, and IP addresses generated from pages of websites. Meanwhile CDPs can store the same information as DMPs, but also very detailed deterministic information on people's profiles and behaviours aggregated from both online and offline sources. These are often generated from purchase transactions, Customer Relationship Management (CRM) database tools or filled forms and can contain data such as purchase transactions, postal addresses, email addresses and phone numbers as well as numerous web behaviours - and very often containing sensitive Personally Identifiable Information (PII). For the purposes of digital marketing CDPs will have to attempt to authenticate any users they have access to online and then also (often via DMPs) make those users addressable via cookie-based advertising platforms.

Market Study: UK Programmatic Supply Chain Transparency Study

Since the release of the first version of the Australian Digital Advertising Practices in 2018, there have been a number of studies and reviews of the digital value chain. In May 2020 ISBA (the UK's advertisers association) in partnership with the Association of Online Publishers published a report into the forensic end to end analysis of the disclosed programmatic supply chain using data supplied by 15 advertisers & 12 publishers. The full executive summary of the report can be found in the Further Reading section. The research conducted by PwC (UK) concluded that a significant proportion of advertisers spend within the study could not be attributed and called for two actions to resolve this. Firstly, an improvement in transparency and standardisation across contractual and technology areas is required to facilitate data sharing and secondly, that all industry participants should collaborate to identify the unattributable costs and agree industry wide actions to identify them. The AANA, IAB & MFA are committed to working together to achieve these outcomes starting with the adoption and broader application of the programmatic standards ads.txt, app-ads.txt, sellers.json and OpenRTB SupplyChain object (all driven by IAB).

VIEWABILITY

THE CHALLENGE

Viewability is often misunderstood. Whilst commonly believed to be a media owner or supply-side problem, it is actually an issue for both the buy and sell sides of the advertising equation.

This means that improvements to viewability and best practice require media owners, creative agencies, media agencies and advertisers to all work together.

The collective pursuit of viewability can have an impact on cost and other digital metrics – but it still remains a valuable metric to strive for.

WHY IS VIEWABILITY IMPORTANT?

For the purposes of this document, viewability is defined as "the opportunity for digital advertising to be seen by a human within a recognised time frame."

Naturally, an ad cannot be effective if it is not seen. However, it is not the only (or even the most important) measure of effectiveness because whilst an ad must be seen to be effective, it does not become effective just by being seen.

WHY ISN'T EVERY AD VIEWABLE?

There are many contributing factors as to whether an ad might or might not be deemed viewable, but most of them relate to humans interacting with an imperfect internet.

Firstly, an ad not being deemed as viewable doesn't mean it wasn't served or that it was not seen at all. Instead it may be that the ad didn't load fast enough and/or only part of the ad was seen.

For that reason, ad load is important. The heavier an ad is, the slower it loads on the page and the less likely it is to be seen because the greater the likelihood the user has moved on.

Ad load or ad file weights have been increasing as more code is 'wrapped' around ads. This code can include creative, interactivity, data integrations, brand safety tags and, ironically, viewability beacons.

Therefore there is a trade-off to be made between the functionality of an ad and its file weight, which in turn affects viewability.

Another consideration is an ads format.

The most viewable ad format is one that obscures the content and/or makes it difficult for a user to move past or dismiss it. Yet this situation would deliver an unacceptably poor user experience and ads of this nature encourage ad blocking. They have also rightly been sanctioned against by the Coalition for Better Advertising and should be avoided.

Larger ad formats may seem more engaging, however the size can lead to a greater likelihood that a number of pixels will be pushed out of view – especially on mobile – which negatively impacts viewability.

Each of these variables can result in a 'non-viewable' ad impression. It's not considered ad fraud as many legitimate factors may be contributing to the issue.

Advertisers, media agencies, creative agencies and media owners need to work together to determine how best to manage and account for viewability according to their campaign's objectives, in balance with engagement and user experience.

VIEWABILITY

HOW IS VIEWABILITY MEASURED?

To measure viewability, independent third-party verification tools including IAS, MOAT, DoubleVerify and inbuilt ad-server solutions (e.g. Active View on the Google platform) are required. These technologies enable advertisers to measure whether an ad is in view or not.

The Media Rating Council (MRC) — a U.S. governing body whose purpose is setting valid, reliable and effective measurement standards for the industry - currently defines viewability as 50% of the ad in view for one second for display ads and 50% of the ad in view for two continuous seconds for video.

Whilst these standards have been generally adopted as a minimum, viewability rates for display and video have improved significantly over the last two years. Many media agencies have developed their own augmented standards, for example that 100% of the ad needs to be in view for three seconds.

According to all viewability vendors, viewability rates for display and video have improved significantly across the market over the last two years.

VIEWABILITY UPDATES

It is vital for all parties to stay up to date with key changes both locally and globally that could influence viewability in the Australian digital ecosystem.

For example, the MRC has been developing new viewability standards to help facilitate cross media audience measurement for video advertising and flagged them for introduction officially from 2021. These standards define the minimum viewability rate as moving to 100% of the ad in view for two continuous seconds for video, as well as the introduction of reporting for duration weighting.

In addition, the World Federation of Advertisers' (WFA) Global Media Charter outlines the 'Eight Principles for Partnership' and calls for action from both advertisers and organisations across the media value chain in relation to viewability measurement. The WFA will also be releasing new principles for cross media measurement in 2020 that will initially focus on cross video (digital video & TV) measurement.

It is vital for all parties to stay up to date with key changes both locally and globally that could influence viewability in the Australian ecosystem. Please refer to page 27 in the Further Reading section for relevant and useful links.

TRADING ON VIEWABILITY?

We need to ensure advertises have the ability to buy highly viewable ads at a reasonable and mutually agreed standard. However, the Australian Digital Advertising Practices do not seek to include policy or propose benchmarks or regulations to viewable trading. This is because there are numerous complications with having a blanket approach to viewable trading, including:

- Supply and demand pressures inflating costs and reducing reach.
- Creative size and weight impacting load times (and viewability as a by-product).
- Different channels, formats and devices having different viewable benchmarks.
- Viewability optimisation undermining key campaign objectives (e.g. sales, cost per acquisition, brand preference etc.).
- Advertisers and agencies having different standards and approaches.
- Different technologies with different methodologies used in measurement.

VIEWABILITY

VIEWABILITY CHECKLIST

1. Choose ad verification technology

Firstly, determine which ad verification technology vendor to use. You will need to understand the pros and cons of using inbuilt ad server solutions (e.g. Google Ad Google Ad Manager's Active View) versus independent third-party verification companies (e.g. IAS, MOAT, DoubleVerify etc.).

There are cost and quality implications to each choice which is why an informed decision based on an advertiser's need is essential. For example, Active View is free and built into the Google technology stack, but it could be perceived as Google marking its own homework. IAS, MOAT and DoubleVerify are all independent third-party vendors, but additional costs and set-up are required for implementation.

You must also consider the impact that multiple tags from ad verification technologies will have on performance. Additionally, for in-app environments (mobile, CTV etc.), app developers should consider using the IAB's OMSDK.

This is because there will always be an increase to the number of tracking tags running on a media sellers' site and multiple vendors means multiple tags – which will have an impact on site performance and costs.

The IAB's Open Measurement SDK (OMSDK) is an in-app solution for advertisers working with a wide range of viewability vendors (such as MOAT, IAS, Google and DoubleVerify). It allows buyers to include third-party viewability and measurement vendors via the one SDK (rather than several), either within bid response fields, or within the creative itself.

2. Define your measurement standards

The AANA, MFA and IAB are aligned to the current MRC standard definition of viewability as a minimum.

The current MRC standard is 50% of the ad unit in view for one second for display. For video, the standard is 50% of the ad unit in view for two continuous seconds. However, a bespoke standard may be a better fit for your campaign.

You should decide on the standard to measure against and ensure that the advertiser, agency and vendor all understand. This is crucial to success.

3. Set measurement benchmarks

Once a campaign viewability standard (e.g. MRC standard or bespoke) is agreed upon, decide on the percentage of digital campaign ad impressions required to meet the agreed standard. This is the percentage of the total number of measured ad impressions in view.

Presently, the AANA states advertisers should expect digital campaigns to have 70% of the ads purchased in view.

4. Ad impressions in view will vary by platform

Remember to factor in platform variance to measurement benchmarks. The percentage of ads in view will vary by channel, platform and execution. For example, video pre-roll is a forced view and will often have a higher viewability score than display or mobile placements. More than one benchmark may be required depending on the channel or platform included in the campaign.

VIEWABILITY

5. Develop creative for the platform

Many viewability issues stem from creative that doesn't fit in with the ad environment, or jars with the user experience , it is important ensure the ad creative is designed for the specific channel or platform. If an ad isn't designed for optimal engagement, viewability benchmarks are unlikely to be achieved. For example, optimising the first five seconds on YouTube or having creative built for the mobile newsfeed on Facebook will likely improve viewability compared to reusing a generic television commercial.

6. Use 'polite download'

Ensure the ad creative is served via a 'polite download'. This means the ad will download in the background while the webpage is being formed, which increases loading speed. This will help improve viewability rates and create a positive user experience.

7. Decide on the 'right' number of tags

Tags are necessary for ad serving, audience measurement, DMP tracking and viewability measurement, but too many tags can increase load times and have a negative impact on viewability.

Be aware of the number and composition of tags attached to creative and how this can impact page performance. If the page takes two seconds to load, the viewability will likely suffer as users might have moved on before the ad appears.

8. Understand the impact of working in-app environments, video and connected TV (CTV) ads

The technical implementation for mobile in-app ad viewability verification is more challenging and has historically been a viewability weak spot for media owners that are not running the IAB's Open Measurement SDK (OMSDK).

Tracking of viewability on desktop activity is generally straightforward with a tick box within the ad server or demand-side platform. On the other hand, video and walled garden activity often requires an additional manual process. Make sure these processes are being followed otherwise activity will not be tracked.

There are technical challenges in tracking viewability of ads being served via over-the-top (OTT) or smart TVs, generally referred to as connected TVs. In this environment, non-measurability does not necessarily mean an ad has not been viewed. It is highly recommended that marketers promote the use of IAB's Open Measurement SDK (OMSDK) for all in-app environments.

9. Stay updated on walled garden policies

There are nuances around what can and can't be measured within certain walled gardens. This will depend on the extent of the integrations that have been implemented by third-party verification vendors.

Have an up-to-date understanding of these limitations and how this will manifest in viewability results.

10. Optimise to viewability at a placement level

When booking a campaign with a vendor, there will often be multiple placements or formats running. One placement may be a highly viewable format and another, below the fold with low viewability. Optimising the campaign at a placement level will ensure the full picture of viewability performance.

Ensure all relevant parties, including vendors, are aware of the agreed optimisation strategies before the activity begins. For example, one vendor may have a high overall viewability score, but some placements could achieve 90% viewability while others achieve 20%. Reviewing on a placement-by-placement basis is required to understand which are delivering maximum results.

VIEWABILITY

11. Sense check viewability standards with campaign goals

Optimising for viewability can sometimes adversely affect key campaign objectives such as brand lift, reach or sales, so it is important to sense-check the viewability standards against core KPIs and business goals.

For example, a campaign that is solely optimised for viewability would likely be overweight in video placements as video is a highly viewable platform. However, as video is an expensive platform, this could impact sales or cost per acquisition campaigns. Similarly, a certain channel, format or site may have lower rates of viewability, but show strong brand lift or preference scores.

In addition, ensure viewability data is feeding through to your attribution models, as creative that hasn't been seen cannot influence consumers.

12. Consider all the digital quality metrics

While viewability is important, there are similarly important digital quality metrics you should factor into a successful campaign.

For example, highly viewable ads in an environment that is not brand safe or appropriate should not have a higher quality weighting over an ad with a lower viewability in a brand-safe and fraud-free environment.

Ensure you consider metrics and parameter like on-target delivery, brand-safe environments and ad fraud-free inventory alongside viewability metrics.

13. Understand the impact of viewability standards on supply and demand

The higher the viewability standard and measurement that you select, the more the supply of inventory will be reduced — which can in turn increase the cost of media and impact performance.

Always factor in performance goals such as sales, cost per action, brand health and lift metrics when planning, buying and optimising for viewability, as it may have a detrimental effect if not considered as part of the wider campaign performance goals.

AD FRAUD AND BRAND SAFETY

THE CHALLENGE

In 2019, online display and video advertising spend hit $3.5 billion in Australia. We know that on average 2-3% of this category of advertising spend is lost to ad fraud, suggesting that in excess of approximately $100m per year is forfeited - a significant figure in anyone's eyes.

While ad fraud has the greatest direct financial impact on advertisers, brand safety has a significant impact as the perception and value of a brand can be eroded by the placement of ads beside content that is deemed unsuitable and, in extreme cases, harmful.

Ad fraud and brand safety are separate and significantly important issues posing a major challenge to advertisers as they consider where to invest their advertising budgets. However, the practices and tools employed to address them are often the same.

WHY ARE AD FRAUD AND BRAND SAFETY IMPORTANT?

Ad fraud is the practice of fraudulently representing online impressions, clicks, conversions or data in order to generate revenue. The impressions that result from intentionally deceptive practices, designed to manipulate legitimate ad serving or measurement processes or to create fictitious activity lead to inflated impression numbers which can skew media results and waste marketing dollars. Publishers are also impacted as they ultimately lose revenue.

There are three key descriptors of ad fraud:

- Invalid Traffic (IVT): Any traffic to a website that is generated, either intentionally or unintentionally, that is invalid. This comes in two distinct forms:
    - General Invalid Traffic (GIVT): Traffic that comes from known non-human sources on publicly available IP lists such as crawlers, proxy traffic, data centre traffic, bots and spiders. These are benevolent (whilst still being non-human) and do not engage with ads. Most ad serving and tracking systems are sophisticated enough to ignore these by default.
    - Sophisticated Invalid Traffic (SIVT): Non-human traffic that is more difficult to detect, is the result of criminal efforts and requires advanced analytics or human intervention to analyse and identify. Examples include malware installed on a computer, hijacked devices, cookie stuffing (the practice of dropping multiple cookies after someone views a page or clicks on a single link) and incentivised browsing.

It may sound complicated but at its most simplistic level, ad fraud involves the gaming of digital advertising, mostly through the use of technology.

Some real-world examples of ad fraud include:

- The delivery of pre-roll video placements in display banner slots.
- Falsifying user characteristics such as location and browser type.
- Hiding ads behind or inside other page elements so they cannot be viewed.
- Selling inventory automatically generated by bots or background mobile-app services.
- Serving ads on a site other than the one provided in a real-time-bidding request, a practice known as domain spoofing.
- Hindering a user's opportunity to engage by frequently refreshing the ad unit on a page.

The real challenge is that there is no way to remove all risk of ad fraud, but it can be minimised.

Brand safety refers to exposure to an environment and/or context that will be damaging or harmful to the brand.

This could be an ad published next to, before, or within an unsafe environment that promotes religious extremism, child endangerment, pornography, drugs or extreme violence.

AD FRAUD AND BRAND SAFETY

It is important to distinguish between websites that feature content promoting these topics from websites that report on them via public interest journalism.

It is an advertiser's responsibility to define what it views as acceptable levels of risk regarding brand safety, where risk is defined as strategic, operational, financial or regulatory.

Additionally, brand suitability must be considered, which refers to a brand appearing in a safe environment adjacent to, before or within content or a domain that is deemed by the brand to be unsuitable. An example of this could be a brand's ad appearing alongside news content that is negative for the particular industry or brand.

Brand safety is important because having an impression in the wrong context may be wasteful, but a potentially harmful impression can also contribute to poor brand perception, diminished brand equity or even lead consumers to boycott the brand and its products.

AD FRAUD AND BRAND SAFETY CHECKLIST

1. Determine your risk areas

Brand safety and suitability are broad topics that cover many different parts of a brand's business. There are a range of factors to consider, including whether advertising falls under certain legislation and regulation.

It is therefore critical to implement a risk assessment, control and action plan for ongoing review which considers the following:

- Define the business's risk tolerance: How much of a problem would it be to have a brand safety incident? What are all the themes which are deemed high or low risk to the brand and what do you consider to be issues? Are there any legal requirements when advertising that you need to adhere to? For example, the exclusion of advertising for gaming and alcohol products or restrictions around advertising to children.
- Complete a risk matrix: Consider the different types of inventory you will be using then assess the technologies available to manage these risks. Identify which stakeholders are required to sign off on the risk matrix.
- Ensure stakeholders understand there is no way to remove all risk: It can only be minimised, controlled and adjusted. Explain the types of risks you may face to various stakeholders — marketing, media, internal communications, legal, chief technical officers and external agencies.

The more risk averse a brand is, the more the opportunity of inventory is reduced. This can limit reach, increase cost for campaigns and also restrict the effectiveness of data being used to target an audience.

2. Determine and document suitable and unsuitable advertising environments

Depending on the risk assessment, control and action plan outcome, some brands may wish to avoid specific environments all together. For example, user-generated environments, native content, app networks and video networks have no way of preventing ads appearing against inappropriate content.

It is advisable to develop a brand suitability playbook which clearly sets out all parameters for new starters and agencies to use.

AD FRAUD AND BRAND SAFETY

3. Measure and monitor

Once a risk assessment has been performed, measuring and monitoring is key to ensuring compliance. All stakeholders, from internal through to media and creative agencies, must be aligned on the assessment and understand what is being tracked and measured; and what the acceptable metrics and standards are.

If all parties are clear on measurement and acceptable metrics, risk is reduced and, if a brand safety incident arises, management of the issue can be expedited.

4. Create an exclusion list to protect your brand's image

An exclusion list, sometimes previously known as a blacklist, is a list of websites and mobile applications which a brand does not wish to advertise on. Typically, an exclusion includes sites and apps that contain inappropriate content, excessive ad placement, deliver poor performance and have high levels of ad fraud.

When developing an exclusion list, advertisers should consider the balance between the cost to brand image from appearing on an inappropriate site versus the impact of reduced reach and the incremental cost of monitoring these sites.

5. Create an inclusion list

Rather than develop an exclusion list, some brands prefer to develop an inclusion list, sometimes previously known as a whitelist, which includes the sites and apps where ad placements can run. An inclusion list gives advertisers the most control and typically includes sites and apps that contain appropriate content, have quality ad placements, have low levels of fraud, a good historical performance and will help protect the brand's image.

Building an inclusion list of long-tailed sites would be resource intense so generally speaking, sites and apps with high audience volumes are recommended for this approach.

This approach is also not recommended for brands looking to target niche content, as it would likely limit the direct response performance of campaigns by limiting reach.

6. Create a negative keyword list

A negative keyword list of explicit terms or 100% unsafe words, should be created to exclude unsafe or unsuitable environments. It should be used in conjunction with an inclusion/exclusion list approach to exclude ads from being triggered by toxic content or placed on sites that hold toxic content categories.

An example of this would be if content on the site refreshes or changes at a regular occurrence, such as a news site. You might choose to avoid negative news such as a terrorist attack or a natural disaster. Ensure you are aware of how often the technology being used scans (also known as 'spiders') the site for content and if the technology is reliant on the site correctly tagging and using metadata for analysis.

It's advisable to manage your keywords in conjunction with semantic contextual tools if possible, so as to fully understand the editorial context, and any associated risk, instead of relying on simple lists of blocked keywords (e.g. 'coronavirus' or 'crash').

7. Create a negative environment list

In addition to keywords, publishers have other filters available to specify the right level of brand suitability for your brand. These can include broader inventory modes, content labels similar to those used in the film industry, as well as more specific topics and categories to be avoided. You are encouraged to consider developing a list which specify specific environments that should be excluded

AD FRAUD AND BRAND SAFETY

in campaigns. An example of a common practice is to exclude mature content, unless the brand specifically wants ads to show alongside more risky content.

As with keywords it's important to document these exclusions to ensure they are used consistently and to keep these lists updated over time.

8. Maintain all your exclusion and inclusion lists

To be effective, exclusion and inclusion lists must be dynamic, being updated regularly to reflect the constant evolution of risks, sites and platforms. Document and implement a process for the upkeep of the lists which might include:

- Setting up a system of review at regular intervals.
- Establishing if URLs that are flagged as fraudulent or not brand-safe will be automatically added to the exclusions list, or if this will need to be done manually. If it will be done manually ensure someone is assigned this responsibility.
- Understanding how exclusion and inclusion lists are applied and verified by agency partners.

9. Set clear guidelines on transparency and accountability

Clear guidelines around accountability and transparency need to be set for every vendor and partner that is involved transacting or ad-serving ad placements for your campaigns. These guidelines should be considered when establishing or reviewing vendor agreements and the onus is on the advertiser to:

- Agree how impressions lists are supplied and when.
- Check whether anonymous/masked URLs are to be blocked.
- Check whether site lists have domain-level transparency and if aggregated exchanges or networks are blocked? Do they need to be?
- Establish a declaration of any guaranteed inventory sources in an aggregated buy.
- Ensure there is the opportunity for any sites to be removed mid-campaign within 24 hours of request.

10. Determine your technology

There are numerous considerations around which technology should be used to combat ad fraud and brand safety issues. These include:

- Agree which ad verification technology vendor to use: Understand each vendor's pros and cons and the cost implications of using their technology.
- Accreditation: Ensure that the vendors you are considering are accredited and meet MRC industry measurement standards for the filtration and disclosure of invalid traffic.
- Is URL analysis needed?: If you want to analyse a site's URL and the page URLs this will be required. For example, a news website may be 95% brand safe but there may be certain articles on the site that are not safe for the brand. URL analysis will help to determine these.
- Will the technology analyse inbound and outbound links?: Inbound and outbound links are sites that link to the page or sites the page links to. For example, a page full of adult images may have no keywords to analyse in the verification process, but the page may contain links to other adult sites that can provide an indication of the content.
- Will the technology conduct metadata (code) analysis?: Metadata does not appear on the page itself but it includes keywords and other indicators in the site code that are important.
- Ads.txt : An IAB-approved text file that aims to prevent unauthorised inventory sales, the ads.txt file lists all of the companies that are authorised to sell a publishers' inventory. Programmatic platforms also integrate ads.txt files to confirm which publishers' inventory they are authorised to sell. The use of ads.txt allows buyers to check the validity of the inventory purchased, however not all publishers have adopted ads.txt so it may reduce campaign reach if only ads.txt authorised sites are used.
- Investigate using pre-bid solutions: As the name suggests, a pre-bid service can assess the brand safety risk ahead of the time of the bid. This can provide additional safety; however, the costs are often much higher and may restrict the reach and performance of the campaign.

AD FRAUD AND BRAND SAFETY

11. Determine your reporting requirements

Ensure reporting requirements are discussed and agreed. This should include a site list for all impressions delivered and you should consider manual URL spot checks pre, during and post campaign delivery.

12. Establish a breach process

Agree on a process to be implemented if a brand safety or ad fraud breach occurs. This needs to cover risk scenarios, stakeholder responsibilities and actions both internally and externally.

13. Sense check ad fraud and brand safety standards with your campaign goals

Optimising for ad fraud and brand safety can impact campaign cost, coverage and reach, so it's important to weight up the benefits of all elements. This includes supply and demand to cost, as well as understanding the percentage of activity that is being run through private marketplace and the open exchange. Buying from open exchanges is cheaper and can be effective, but there is more possibility of ad fraud or brand safety issues.

14. Define the billing process

If booking through an agency, the billing process will depend if an advertiser has a "guarantee outcome based model" or "itemised model" (sometimes referred to as undisclosed and disclosed models) arrangement with their agency. See page 5 in the Digital Value Chain module for more details on this.

DATA GOVERNANCE

THE CHALLENGE

Determining the quality and provenance of data acquired for marketing is tough because the landscape is complex, driven by its rapid growth and hampered by a lack of local legislation. Available data sets vary significantly in terms of the data utilised, the approach to construction and the cadence of refresh.

This represents a challenge to advertisers and media buyers, who then have to unpack the varying propositions in market and determine the relevant value to their marketing efforts.

WHY IS DATA GOVERNANCE IMPORTANT?

Understanding the governance of a data set and how it has been created, is important both from a value (to the advertiser) perspective but also, in this rapidly changing world, its long term usability. The value of a data set is specific to an advertiser and their intended use of the data within marketing plans. For example, an advertiser whose product has an intent window of hours (e.g. FMCG advertiser), the cadence of data refresh is likely to be a priority. For this advertiser a data set that is refreshed every 30 days may hold little value.

Further, with the upcoming review of the Australian Privacy Act throughout 2020 and 2021 as well as a variety of international regulation changes (e.g. GDPR, CCPA), advertisers will have to ensure the data being acquired is legally compliant and that it will also be usable in the trading platforms in the future.

WHAT TYPES OF DATA ARE THERE?

First-Party Data

First-party data is your own data. It includes the information you collect directly from your customers, such as: data you have in your CRM, your subscription data, your own social media data, etc. As this is data that you collect directly from your customers or target audience, it is typically accurate, relevant and presents the least privacy concerns because you have full control over its collection, ownership, and use.

Second-Party Data

Second-party data is another company's first party data that has been shared for the purpose of creating audience segments or insights for the brand's use. Second-party data can be purchased directly from the company that owns it, or can be found through a data co-op. It often includes the same type of information you could collect as first party, including website activity, customer surveys and location data. As you acquire this data directly from its owner, it is important to evaluate its attributes, quality and privacy compliance. The value of second-party data is that it allows you to access data that you do not have available as first party and because you establish a direct relationship with the data provider, you are typically able to evaluate and control its quality and privacy compliance in more detail.

Third-Party Data

Third-party data is data that has been sourced and aggregated by a company that was not the original collector of the data and then made available for sale to a brand or platform. This data may include demographic and psychographic data, intent, and online and offline interests. A key advantage of this type of data is that it allows you to amplify the scale and scope of your own first party data. For example, marketers can use third-party data to build upon their audience segments and deepen the understanding of their interests and behaviours.

Personally Identifiable Information (PII)

This refers to information used or intended to be used to identify a particular individual, including name, address, telephone number, email address, financial account number, and government-issued identifier.

DATA GOVERNANCE

For legal purposes the Australian Privacy Act defines personal information as:

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.

Cookies

Also known as an HTTP cookie, web cookie, or browser cookie, this is a string of text sent from a web server to a user's browser that the browser is expected to send back to the web server in subsequent interactions. A cookie has a few core attributes: the cookie value, the domain and path within which it is valid, and the cookie expiry. There are other attributes as well that limit the cookie to https-only transactions or hide it from JavaScript.

The domain and path define the scope of the cookie – they tell the browser that cookies should only be sent back to the server for the given domain and path. Cookies that do not have a specific expiration date and time are automatically deleted when the web browser is next closed. Cookies with a set expiry time are considered persistent cookies, while cookies without set expiry times are considered session cookies.

In online advertising, cookies generally store a unique identifier, and may contain information like what ads were recently seen (for frequency capping), when the cookie was created (to discover short duration identities), and other simple attributes.

Changes in browser tracking continue to roll out across the industry with Google announcing that Chrome will no longer support third party cookies within two years. This change follows similar moves from the FireFox browser and Apple for the Safari browser. These changes will have a major impact on much of digital marketing from analytics, targeting, measurement and attribution. The industry is now working on new privacy complaint approaches.

For more definitions please refer to the IAB glossary of terminology.

DATA GOVERNANCE CHECKLIST

1. Has the data been gathered with genuine consent?

Although consent isn't currently mandated within Australian legislation, the expectation is that local legislative changes will at some point mandate that user consent must be provided to utilise consumer data for advertising. To set your business up for success, and to ensure that your own data strategy meets local legislation it is worth establishing if the data sets you are currently on-boarding have been gathered with user consent. When GDPR was introduced within the EU, many advertisers found that the data strategies that they had become reliant on had to be completely reinvented in light of the new legislation. Asking how your data set has been created will help you understand the proportion of your data that will need to be reviewed should legislation change in the coming months.

2. Who owns the data set?

Data sets are sold by many means. At times sellers sell access to their own first party data sets and also have the potential to act as data resellers where they have brokered partnerships with other data owners to on-sell partner data. For example Nine on-sells its own first party data and they allow advertisers to purchase Red Planet (Qantas) data sets and also combined Nine and Red Planet data sets. Understanding the origins of the data sets being used will helps you understand the ownership that the vendor has over the data, the construct of the data and the potential usage limitations placed on the data set in question.

DATA GOVERNANCE

3. Where is the data stored?

Understanding data storage will help you understand if the data is in a format that suits the business purpose for which it is intended but also its suitability for your own business. Some sectors (such as Finance) requires certain data types to be stored on-shore versus offshore.

4. How has the data set been constructed?

Each data set construct is unique, however there are some key factors that you need to understand as these factors will determine the value of the data set to your business.

- Refresh cadence: There is little standardisation when it comes to refresh rates, however the cadence is key to the business suitability, which will dictate how long or short the refresh rate should be. A comparable example is a consumer journey, which varies significantly by the product or the brand in question. The same can be said for data sets.
- Audience size: The size of an audience will provide indicators as to the nature of the data set and the value to your business. For example, if an audience size is significantly larger than the known population of your people-based audience, it is more likely that your data set has either been modelled or augmented in some way and look-a-like audiences will have been used. Similarly, if an audience size is low versus your target audience, then this will allow you to understand if the data set itself is going to be usable in different buying platforms where the data will require matching.
- Data Type: There are many varying types of data. Depending on your business base for the data utilisation you may require a specific type of data to complete your desired application. Prior to transacting you should understand the types of data sets that have gone into constructing any single audience.

CREATING MARKET STANDARDS

In September 2019, IAB Australia launched the Data Label initiative with the intention to establish a set of standardised minimum disclosures and transparency criteria for any company that collects audience data for targeting, personalisation, or measurement of digital advertising, and ultimately to encourage more education and informed data usage.

Learn more about the IAB Data Label and Transparency

CONSUMER PRIVACY

WHY IS CONSUMER PRIVACY IMPORTANT?

Consumer trust is the lifeblood of digital media. This means that it is imperative to safeguard the personal and confidential data of customers, employees and business partners.

Maintaining best practices of privacy and security controls to comply with the law reduces the chance of reputational damage from a data or cyber breach, strengthens the business by increasing consumer confidence and better manages post-breach incidents.

If you are collecting or processing data on consumers in other geographic markets it is essential that you are across the law in each country including the well-publicised roll out of General Data Protection Regulation (GDPR) and the roll out of the Californian Consumer Privacy Act (CCPA) in early 2020. There are many other countries currently reviewing their privacy regulation particularly in relation to the marketing industry, including Australia.

CONSUMER PRIVACY CHECKLIST

1. **Manage consumer consent and control: champion the user experience**

It's essential you determine the controls to give to customers when it comes to consent. Under Australian Law, personal information collected by an entity may only be used or disclosed for the primary purpose for which it was collected, unless an exception applies.

This means the way personal information is collected, and what the individual is told about the collection, is important for data activities. Businesses should implement the Office of the Australian Privacy Commissioner's (OAIC) Privacy Management Framework which encourages the use of a Privacy Impact Assessment (PIA), to inform big-data activities. This includes mapping the information life cycle, identifying what personal information is collected, whether it might be utilised for big data and for what purpose. Undertaking these steps will inform what personal information should be collected, how it should be collected and what notice should be given.

2. **Proactively manage privacy protections: be forward thinking**

The Australian Privacy Act requires Australian companies to implement data practices, procedures and systems to ensure ongoing compliance with Australian privacy law. This means compliance is a dynamic and ongoing process. When collecting data on a consumer, the collector becomes a custodian of that data.

The Office of the Australian Privacy Commissioner requires the consideration of privacy and data protections throughout the data life cycle including when:

- Existing owned data is used for new purposes.
- Collaborating with vendors (such as CRM, marketers, or cloud IT providers) that involve data sharing.
- Staying up to date with newly introduced legal requirements (like those introduced in early 2018).
- Developing internal policies or strategies with privacy implications.

Practice data minimisation

3. Under Australian Privacy Law, companies are required to actively consider whether they are permitted to retain personal information. When a business no longer needs personal information for any purpose for which it may be used or disclosed, the company must take reasonable steps to destroy or de-identify personal information.

Best practice guidance on de-identification has been compiled by the OAIC and can be found on the IAB Australia website.

CONSUMER PRIVACY

4. Ensure compliance with data breach laws

New data breach laws introduced to Australia in February 2018 are very similar in substance to new data breach requirements in place in Europe under the General Data Protection Regulation (GDPR). These data breach laws force any company in the digital advertising ecosystem — advertiser, agency, digital publisher or ad tech — to notify all affected individuals and the Office of the Australian Privacy Commissioner if they experience a data breach which poses a risk of harm.

Minimise the risk of a data breach through the following techniques:

- Educate employees: The often used example of a misplaced company laptop can lead to a data breach of hundreds of clients' data. Teach staff the most secure ways of data sharing and storing and how to identify and deal with data breaches.
- Evaluate technology: Check if existing software and hardware can adequately identify and deal with data breaches in real time.
- Minimise the amount of personal information held: This can be a tough one, especially when it comes to advertising databases, but where possible, try and decrease the personal data stored. For more guidance on this, see the resources below.
- Encrypt and anonymise personal data and information where possible.

5. Manage data protections in your advertising tech stack

Any vendor in the digital ecosystem that is processing customer data is liable for the protection of data used. Many marketing professionals rely on third-party vendors (such as CRMs, email service providers, cloud IT services) to interact with customers.

The owner of the first-party data is responsible for speaking with third-party partners processing customer data to ensure they are taking the proper steps to remain compliant with privacy law. This includes having the tools in place that will allow vendors to both retrieve and destroy data at the end of its life cycle.

6. Ethically and transparently sourced data

A whole-of-cycle view of data with deep insight into how and why data is being used is essential for ensuring the right balance between compliance, privacy and innovation.

The revelations around U.K. firm Cambridge Analytica in 2018 demonstrate that it is not good enough to think about data sharing in a linear way. Anticipate any risks that might be involved in the processes employed. Ethical decisions around the use of data will be expected of the company when handling customer data – but don't expect these requirements to be spelled out in every case.

FURTHER READING

DIGITAL VALUE CHAIN

Video Ad Serving Template - Update (Sept 2019)
https://www.iabaustralia.com.au/research-and-resources/research-resources/item/12-research-and-resource/2804-vast-4-x-omid-simid-iab-tech-lab-updates-august-2019

Open RTB Standards - Update (Sept 2019)
https://www.iabaustralia.com.au/research-and-resources/research-resources/item/12-research-and-resource/2803-open-rtb-update-iab-tech-lab-sept-2019

Header Bidding & Auction Mechanics Handbook (Feb 2019)
https://www.iabaustralia.com.au/research-and-resources/research-resources/item/12-research-and-resource/2667-auction-mechanics-dec-2018

IAB Programmatic Playbook
https://www.iabaustralia.com.au/research-and-resources/research-resources/item/2391-programmatic-playbook-oct-2017

Updated Creative Guidelines and Specifications
https://www.iabaustralia.com.au/iab-creative-assets/assets

IAB Industry Open Measurement Project (OM SDK)
https://www.iabaustralia.com.au/research-and-resources/research-resources/item/12-research-andresource/2569-open-measurement-sdk

Advertising Creative Guidelines - Updated for HTML5
https://www.iabaustralia.com.au/research-and-resources/research-resources/item/12-research-andresource/2608-advertising-creative-guidelines-updated-for-html5

Mobile Best Practices Handbook
https://www.iabaustralia.com.au/research-and-resources/research-resources/item/12-research-and-resource/2832-iab-mobile-best-practices-handbook

Native Advertising Handbook
https://www.iabaustralia.com.au/research-and-resources/research-resources/item/12-research-and-resource/2846-native-advertising-handbook-2020-update

IAB Australia Technology Purchase Guidelines
https://www.iabaustralia.com.au/research-and-resources/research-resources/item/12-research-andresource/2447-advertising-technology-purchase-guidelines-mar-2018

ISBA Programmatic Supply Chain Transparency Study
https://www.isba.org.uk/knowledge/digital-media/programmatic-supply-chain-transparency-study/

VIEWABILITY, BRAND SAFETY & FRAUD

MRC standards and definitions
http://www.mediaratingcouncil.org/063014%20Viewable%20Ad%20Impression%20Guideline_Final.pdf

Introduction to ads.txt and app-ads.txt to help fight fraud
https://www.iabaustralia.com.au/ads-txt

FURTHER READING

AANA viewability position
http://aana.com.au/knowledge/resources/aana-launches-paper-ad-viewability/

Viewability whitepaper - IAB
https://www.iabaustralia.com.au/guidelines-and-best-practice/guidelines-best-practice/item/3-guidelines-and-best-practice/2244-iab-viewability-whitepaper-dec-2016

DATA & CONSUMER PRIVACY

Data Label: Adopting data transparency standards for digital marketing in Australia
https://www.iabaustralia.com.au/research-and-resources/research-resources/item/12-research-and-resource/2804-vast-4-x-omid-simid-iab-tech-lab-updates-august-2019

The GDPR and Data Privacy: IAB Briefing and Resources
https://www.iabaustralia.com.au/research-and-resources/research-resources/item/12-research-and-resource/2591-the-gdpr-and-data-privacy-iab-briefing-and-resources

Coalition for Better Ads
https://www.betterads.org/

Regulation Update: New Mandatory Data Breach Notification Laws
https://www.iabaustralia.com.au/guidelines-and-best-practice/guidelines-best-practice/item/3-guidelines-and-best-practice/2410-2396-iab-australia-regulation-update-new-mandatorydata-breachnotification-laws

The Australian Privacy Act
https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australianprivacy-principles

Privacy Management Framework
https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework

SINGLE-PAGE CHECKLIST

DIGITAL TRANSPARENCY CHECKLIST

1. Understand the technology that is currently in place
2. Identify how each component of your digital setup is adding value
3. Examine and decide on media buying objectives
4. Determine the best buying method to meet your needs
5. Determine the base technology you need to meet your requirements
6. Decide what additional technology will add value
7. Choose metrics to track outcomes

VIEWABILITY CHECKLIST

1. Choose ad verification technology
2. Define your measurement standards
3. Set measurement benchmarks
4. Determine if different benchmarks are needed per platform
5. Develop creative for the platform
6. Use 'polite download'
7. Decide on the 'right' number of tags
8. Understand the impact of in-app environments, video and connected TV ads
9. Stay updated on walled garden policies
10. Optimise to viewability at a placement level
11. Sense check viewability standards with campaign goals
12. Consider all the digital quality metrics
13. Understand the impact of viewability standards on supply and demand

AD FRAUD AND BRAND SAFETY CHECKLIST

1. Determine your risk areas
2. Determine and document suitable and unsuitable advertising environments
3. Measure and monitor
4. Create an Exclusion List
5. Create an Inclusion List
6. Create a Negative Keyword List
7. Maintain your Exclusion and Inclusion Lists
8. Set clear guidelines on transparency and accountability
9. Determine your technology
10. Determine your reporting requirements

DATA GOVERNANCE CHECKLIST

1. Has the data been gathered with genuine consent?
2. Who owns the data set?
3. Where is the data stored?
4. How has the data set been constructed?

CONSUMER PRIVACY CHECKLIST

1. Manage consumer consent and control: champion the user experience
2. Proactively managing privacy protections
3. Practice data minimisation
4. Ensure compliance with data breach laws
5. Manage data protections in your advertising tech stack
6. Ensure data is sourced ethically & transparently

Australian Digital Advertising Practices: 2020 Update

This document has been prepared by the Australian Association of National Advertisers (AANA), Interactive Advertising Bureau Australia (IAB) and the Media Federation of Australia (MFA) as a resource for the Australian advertising industry. For more information or assistance, please contact the following:

AANA

admin@aana.com.au
+61 2 9221 8088

IAB Australia

iabaustralia@iabaustralia.com.au
+61 2 9211 2738

Media Federation of Australia

mfa@mediafederation.org.au
+61 2 9282 9634


AANA


iab.
australia


mfa
media federation of australia