1st party *data handbook.*

iab australia

contents.

Welcome to the IAB Data Council's *1st Party Data Handbook*. This is in fact the *third* iteration of our Data Handbook that we've released as I'm sure you can appreciate the need to consistently review and update material as it relates to data in our industry.

The handbook has a specific focus on 1st Party Data and there is no denying how prevalent this topic has been over the past couple of years.

A lot has changed, and a lot will continue to evolve in this space as Brands continue to try and capitalise on the opportunities it represents. I'd like to extend a huge amount of thanks and appreciation to all of our Data Council contributors; for taking the time to craft a compelling update for our industry.

We've all been particularly passionate about collating the most relevant information for you - we hope it's valuable!

If you have any suggestions or feedback on this handbook, please always feel comfortable reaching out to us directly by email at iabaustralia@iabaustralia.com.au

Alison Costello
National Head of Digital
OMD Australia
IAB Australia Data Council Chair

Data and Privacy *Contributors*.

Amy Jansen-Flynn
Adform

Emmalee Crellin
Yahoo

Dan Cravero
Oracle

Tasneem Ali
PureProfile

Laura Kleiman
Crimtan

Richard O'Sullivan
InMobi

David Raitt
Near

Alison Costello
OMD

Greg Kearney
Suncorp

Joanna Georges
The Trade Desk

Moritz Von Sanden
Audience360

Alicia Placer
Blis

Chris Brinkworth
Civic Data

Rick Knott
Infosum

Tim Lillyman
Xpon

Manuela Cadd
Criteo

Chloe Fisher
Liveramp

Alex Melville
Google

Nico Celedon
Google

Introduction

The purpose of this collaborative document **is to provide an updated definition of 1st party data, insights into the various types and formats that exist.**

Please note, this handbook is an IAB document and its contents are not reflective of any particular company's policies. Rather, it is a collaborative effort of the members of the Data Council.

Alongside this you'll find some simple but meaningful examples of the options for both buyers and sellers to effectively maximise, enrich and utilise these assets competently and responsibly for advertising.

We've also worked hard to include as much information on the latest standards in this area as possible and provide some objective guidance on what the various forms of data clean rooms currently look like.

When reading this it will soon become obvious that the content is taken from a wide range of contributors (18 in total!). As these voices come from across different vendors, publishers, agencies and brands – we feel that it's highly representative as a result, but may feel somewhat disjointed when consumed in one sitting.

This is difficult to avoid in such outputs, but hopefully the content remains useful and can be reference on an ongoing basis, along with other recent productions from the IAB Australia Data Council such as the Contextual Targeting Handbook and the Identifiers & Identity Management Explainer.

We will continue to produce these types of collaborative handbooks, look to learn from one another and endeavour to keep the industry updated on any latest changes, requirements or best practices on a regular, basis through blogs, events and outputs such as these.

Please also be aware that most of the case studies in section 7 are hosted and the links embedded in the document will send readers to the hosted documents for further reading or else to the source page of the contributor.

Definition of 1st Party Data & Examples

Section 3

First-party data
is information that is
captured with direct consent
from customers who interact
with your business *online or offline*.

By visiting your website, making a *phone call, signing up for a loyalty program or subscription, or purchasing from one of your stores.*

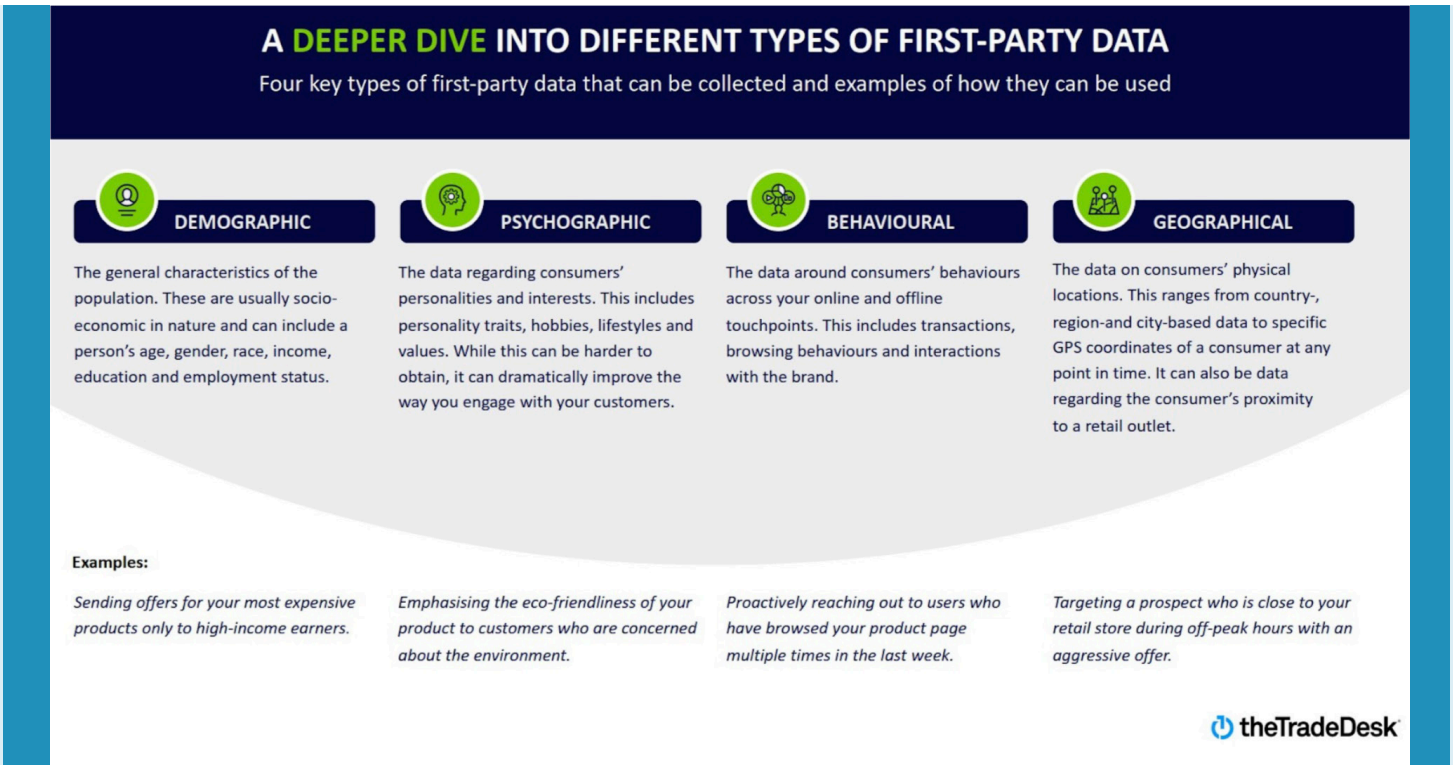
Digital media innovation, progress and focus on privacy has brought the industry to 1st party data and by extension, 2nd party data with trusted partners. First party data is not new, it has been around before the 3rd party cookie. Therefore, it is important for us to understand the difference between the three.

Digital advertising industry is facing one of the biggest changes since banners ads started to show across the web in 1994, with the continued depreciation of cookies across browsers. What has closely coupled digital advertising since its inception is 3rd party cookies. Initially 3rd party cookies were used for verified measurement of impressions and clicks. However, as digital advertising grew in sophistication, 3rd party cookies started to evolve from measurement to audience tracking and targeting.

In the process this made digital advertising one of the most targeted and accountable channels of advertising. However, by nature 3rd party cookies are designed to allow 3rd parties to collect data or track behaviour of consumers on the publisher site, and across any other site they have their tags on.

As the demand for more targeted and personalisation of ads increased, the more fundamental issues around consumer privacy and rights started to gather momentum. The culmination of these issues have led to legislative changes across Europe (GDPR), and California (CCPA), which focused on giving consumers the right to know who collects their data, what it's used for, and allow consumers to opt-in if they trust the provider.

An example of 1st party data in use is when users come back to their favourite streaming service and the log-in details are remembered. The 1st party data stored by this streaming service on the users device ensures that we don't have to re-enter all of our details every single time and it also allows the website to put checks in place that can verify that the users identity hasn't been stolen.



For more than a decade brands (both marketers and media owners) have talked about improving the customer (or consumer) experience. While efforts to improve customer experiences are typically focused on the most high-value touch points, as digital touch points continue to rise and consumer buying journeys occur across multiple devices, focusing on the most important touch points isn't enough. Marketers need to provide better and more consistent user experience across all touch points.

Better customer experiences demand better data

Brands must understand individual consumer and audience patterns which include different channel interactions and their role in the buying journey. They need to know what consumers want, and of equal importance when they want it.

First-party data is the most useful way to connect online (and offline) journeys. Due to ongoing changes in the industry focused on preserving consumer privacy, third-party data (third-party cookies) will no longer be a method for brands to run addressable advertising campaigns. They'll need to leverage first-party data, and work with partners that can help them activate their data at scale, if they want to continue achieving desired outcomes.

Brands understand that first-party data is provided by customers because it helps provide more contextually relevant experiences.

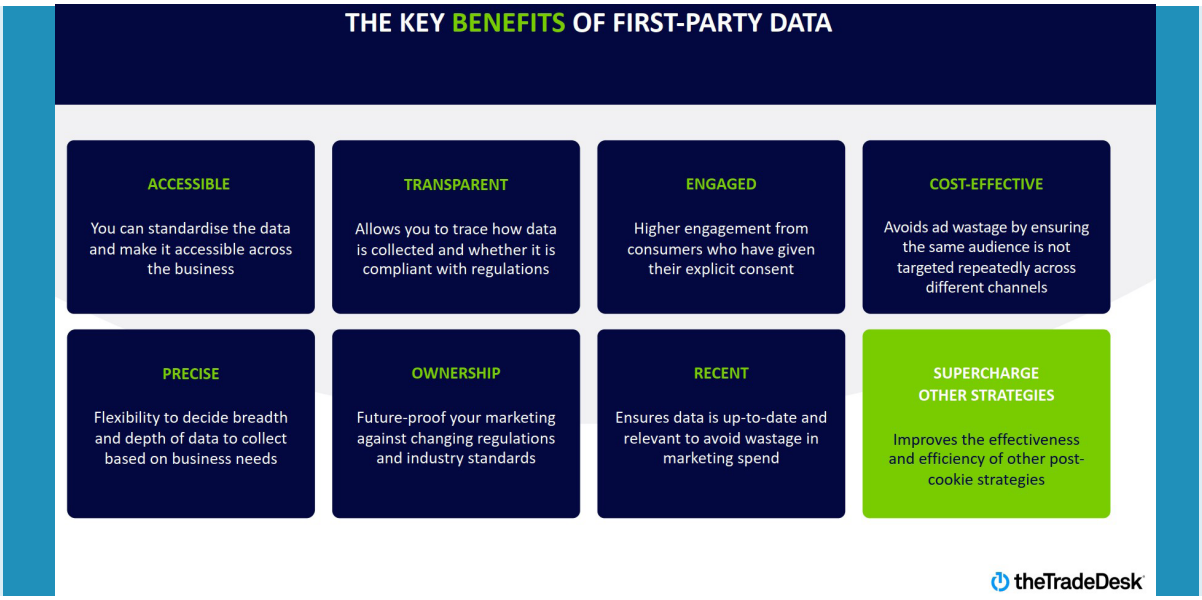
Some examples of these are:

- Receipts of purchase
- Delivery Tracking
- CRM
- Loyalty offers
- Curated email communications populated by previous user interactions
- Curated web/app experiences

Use cases for marketing using first-party data:

Some examples of these are:

- Create single view of the customer
- Improve targeting and personalization through relevancy
- Improve omni-channel measurement
- Map customer journeys
- Close the loop on attribution
- Understand ROI and incrementality



Zero-party data has become an increasingly used term for first-party data which consumers are intentionally and openly opting into sharing with business entities. Technically and legislatively this remains first-party data and any distinction is effectively redundant, other than for product marketing purposes.

2nd party data has the same attributes regarding transparency and trust as first party data but is utilised by a trusted partner of the original provider. An example of a 2nd data partnership is Audience360 who leverage exclusive and direct partnerships with some of Australia's top brands. The benefit of a data partnership is that it allows brands like Webjet to focus on what they do best and enable brands like Audience360 to act as their trusted partner in the area of their expertise.

1st and 2nd party data ensures that only the website and truly trusted partners and the user benefit from the data, and no other 3rd party vendor that may be collecting data covertly, which the user has no knowledge of. By nature 1st and 2nd party data is more transparent, as it's governed by the websites privacy policy and by listing the site or using its services the user has agreed to its terms and conditions around use of the users personal data. This again is in contrast to 3rd party cookies, where the user doesn't have this visibility.

3rd party is when the identifier collected is collected by services which are third party to the website the user is visiting. These are used by 3rd party providers of advertising, retargeting, analytics and tracking services.

BCG research: consumers that trust a brand are twice as likely to share email data.
1st party itself is not privacy preserving, it still requires the website to be transparent with the users around the usage of the data. We have seen attempts of this through GDPR, where websites are transparent around who is collecting the data and why. Furthermore, the website needs to establish a meaningful connection with the customer to build trust. Building meaningful connections can be interpreted differently for different websites.

These are websites where consumers can build trust via the exchange of value. Additionally, there are also websites with which the consumer is not directly exchanging value and rather is consuming snack bite-sized information. Regardless of the value exchange between website and consumer, the key element of trust is ensuring that websites have clear declaration of what is collected, what is the intention of its use and provide users with the option to either opt-in or opt-out, whilst persistently respecting the consumer's decision.

Further Considerations

As an industry we regularly need to remind ourselves that 1st party data is not the silver bullet, we only need to look at the challenges around privacy faced by the walled gardens, who have an abundance of 1st party data.

There needs to be broader regulatory changes to implement transparency and trust around usage of data and most importantly push around consumer education, to allow all consumers to understand this complex topic and make right choices for themselves.

We need to do a better job of educating consumers about value exchanges and we need to collectively overcome technical challenges that may not always accurately represent the pathways and grading of data.

One of the most important topics in the discussion on 1st party data and 3rd party data is economic impact. On revenue alone, digital advertising is a **$455bn industry** which funds businesses that keep information free and accessible for all consumers. It also employs millions of people across the globe and provides a unique way for small businesses to scale their businesses.

A lot of this has been built on the backbone of 3rd party cookies, so as 3rd party cookies deprecate and are replaced by first party cookies, we all need to find a technological and regulatory ground which helps preserve the privacy of consumer online, which still fosters growth and innovation in the digital advertising sector. With this in mind, Audience360, as one of Australia's leading first party data companies, is focusing on three core pillars to create a better internet for both brands and users.

1. Data Transparency:

An actual broad understanding of how data is collected,where data is going and how data is applied can only be achieved through transparency.

Transparency will be a vital communication building block for end users to acknowledge the value exchange in place that allows advertising to pay for the internet.

Transparency will also be key for marketers to have faith in their strategies to ensure their campaigns are engaging with relevant customers. The most promising initiative for this is the IAB data label.

Audience360 is acting as the foundational launch partner on this project, which will give media planners/buyers/strategists a nutrition label style information document to quickly and easily identify what type of data is being presented, where it comes and how recently it has been refreshed.

2. Privacy-first audience targeting capabilities:

Building audience targeting capabilities on the back of cookies wasn't the original intention of cookies so, it shouldn't be surprising that new technology is now created. New technology needs to consider consumer privacy as well as usability to ensure that users feel comfortable with the value exchange and brands can still leverage the beneficial opportunities that audience targeting presents.

The most interesting space to watch in this field are the various ID solutions that are currently popping up and whilst this is a constantly evolving space, there is already some great progress being made to ensure the new way of reaching targeted audiences, doesn't just repeat past mistakes. As it stands in early 2022, Audience360 has successfully leveraged ID solutions to reach 1st party audiences in cookieless environments and is a space that Audience360 will continue to lead the way in.

3.Audience insights and data collection:

Whilst data activation is changing, what hasn't been fully realised is the insights that can be derived from media audiences that can be leveraged across other marketing channels. There are beginning to be signs of **DOOH** leveraging digital signals to inform their site activation strategies.

Some companies have already started leveraging 1st and 2nd party data to educate their intelligent bidding algorithm but all of this is still a very new and exciting industry with lots more on the horizon.

Data Collection

Section 4

Build insightful first-party data from *your customer relationships.*

It's important that you have the tools in place – and permission where required – to generate insightful and actionable first-party data when those direct interactions might take place. Generate first-party data from site visitors: Investing in a strong tagging infrastructure, or sitewide tagging, is a key step towards building a privacy-safe measurement strategy.

This type of approach will be required for the majority of future measurement solutions and will allow you to make the most of the data customers share with you, by setting first-party cookies to measure conversions

Generate first-party data from site visitors

Then, import your offline conversions to measure campaign performance with your advertising and measurement tools including Search where possible.

When first-party data is accurately collected and managed through an accurate consent management workflow, it helps enterprises to build the most effective marketing with their first-party data strategy. Many enterprises face data quality issues hindered by a lack of identity resolution and consolidation, resulting in disconnected customer experiences due to data siloes and fragmentations.

Resolve consumer touchpoint fragments with person-based identity graphs by creating a privacy-centric, durable identity that is convertible across offline, online, and collaborative data ecosystems.

Generate first-party data from app users:

Add a software development kit (SDK) to your mobile app that's designed to help you gather information from the actions people take when they download and engage with your mobile app. You can do this with common Analytics solutions that are available for your Android and iOS apps.

Generate first-party data from offline touchpoints:

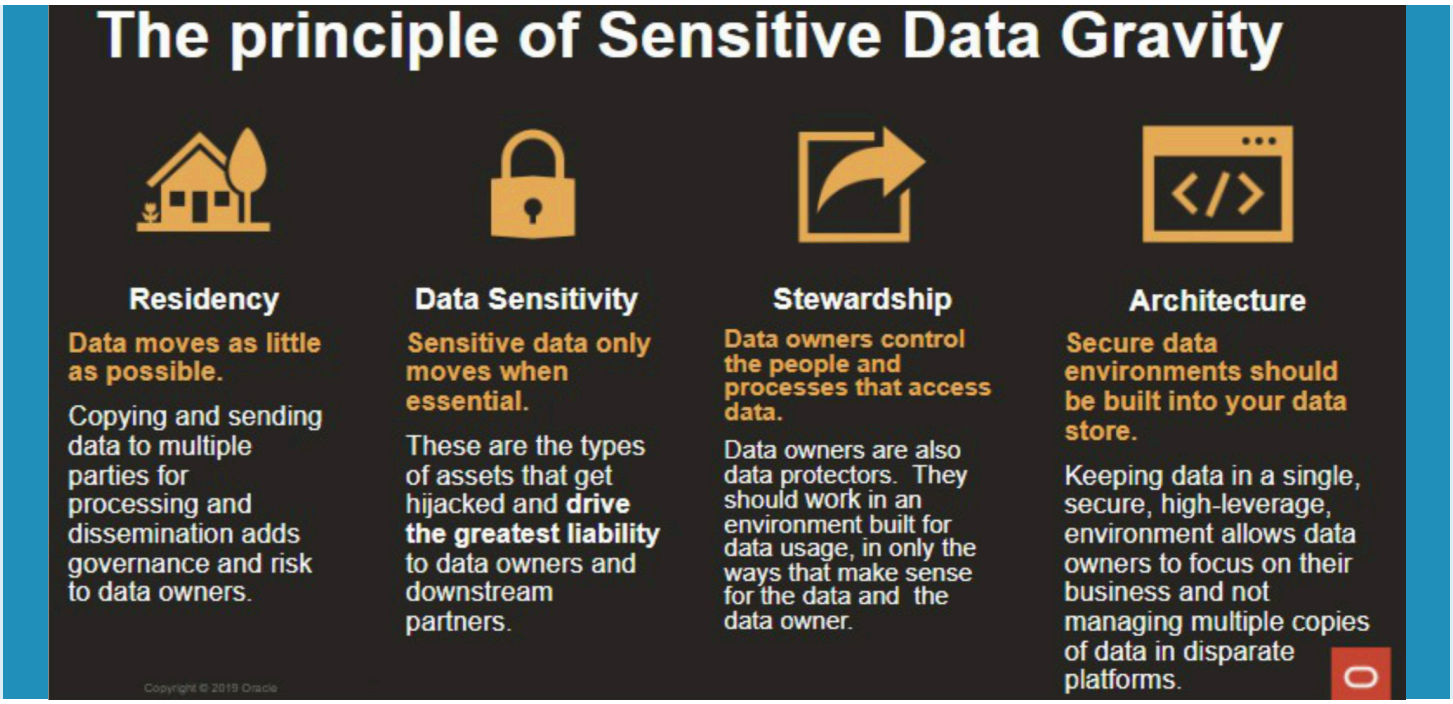
Invest in a customer relationship management (CRM) tool to help you collect and organize the information that's shared by people during offline interactions like meetings or phone calls. Then, import your offline conversions to measure campaign performance with your advertising and measurement tools

Consumers can interact with a brand via multiple touchpoints which include *websites, apps, physical retail locations, social media channels and more.*

This *'first-party'* information is available across siloed data sources such as *apps, websites, CRM, and loyalty systems.*

However, the identities of the customer across these various touchpoints is often varied and this makes it difficult for the brand to get a unified view of the customer. Therefore, without a way for identity resolution, brands are unable to use this rich first party data to its potential.

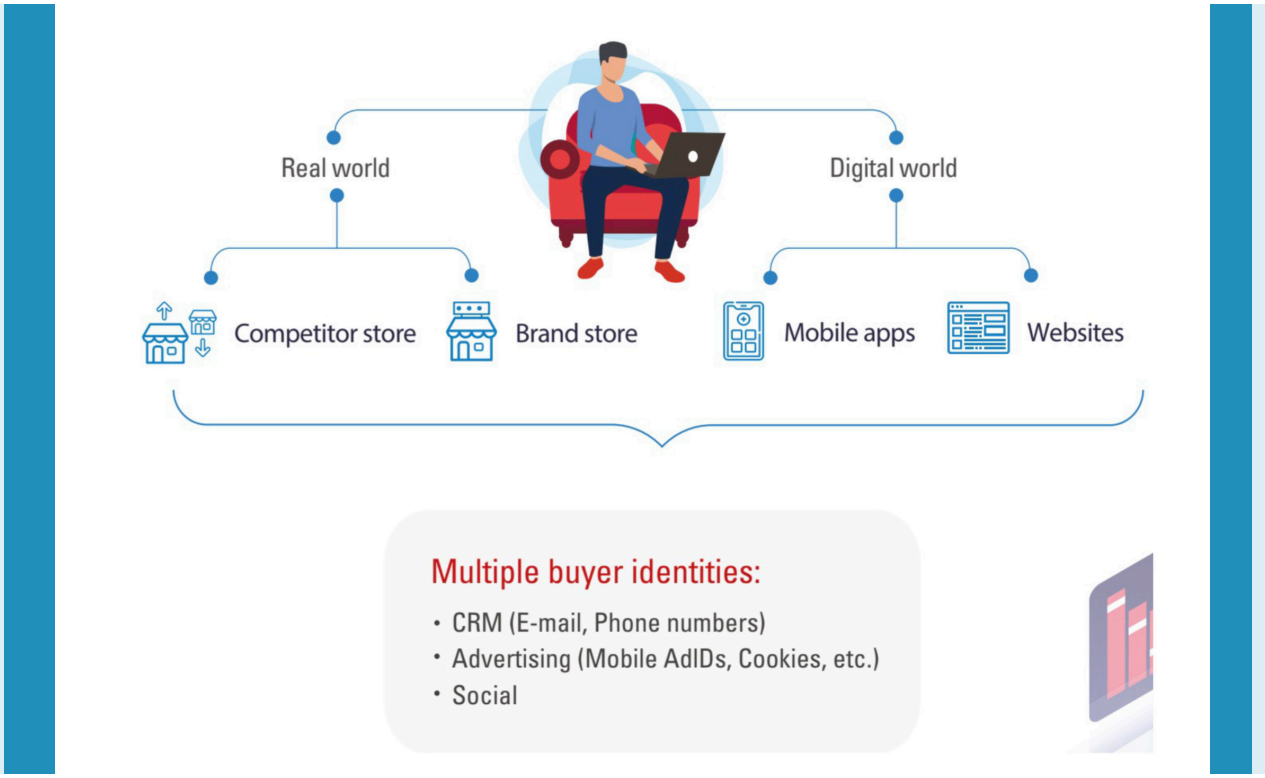
Persistent identity solution helps brands to retain the data already collected, remove redundancy, and then stitch it together. This also opens doors to unlock the value of other third-party data sets that can be used to enrich the existing first-party data and thus develop a data-driven strategy.



sourced from **Oracle**

Identity resolution for a Post-Cookie and Post-Mobile Ad Id world

Out of many solutions available to manage consumer identity across multiple touchpoints, none are seamless enough to mitigate the risks brought in by the recent developments in the online world. For example, Near has recently developed its identity graph called PROXIMA for a post-cookie, post Mobile Advertising ID world.



sourced from **Near**

Solutions such as these can provide a persistent identifier for individuals by connecting various real-world and online signals of consumers using data from various sources like hashed emails, mobile numbers, IP addresses and more. The plurality of signals used makes the persistant IDs resilient even in the absence of curtain parameters such as mobile advertising IDs (MAID) or cookies, as the identity can be resolved by leveraging the other signals available.

Ever since the EU released GDPR guidelines, discussions about privacy have been at the forefront of all partnership discussions. Many companies now utilise a 'Privacy by Design' framework while developing any data platforms, so as to not only ensure that the data received is consented to, but also to make sure that appropriate notifications and opt-out mechanisms are shared with the end consumer.

Enrichment & Management

Section 5

Brands and media owners are always seeking additional consumer data to better *understand, profile and segment their audiences.*

First-Party data enrichment:

Companies can onboard their first party data using various user identifiers such as hashed emails, phone numbers, mobile advertising IDs and cookies.

Identity resolution algorithms can connect multiple IDs to an individual and enriche it with additional data attributes.

The enriched dataset can be used for better customer segmentation, acquisition, and personalization.

Competitive analysis

Compare footfall trends, cross visitation behaviour, and market shares to gain a competitive advantage.

Use competitive intelligence to identify demand patterns and re new customer acquisition strategies.

Store planning:

Location-based data intelligence can help companies plan where to open new stores and where to close existing stores based on footfall trends of their stores and their competitors' stores, the path to purchase, and the demographics and social demographics within a trade area.

Data-Driven Marketing:

Feed actionable insights into their marketing strategy to increase ROI and measure campaign effectiveness by tracking incremental footfalls.

Prospecting:

Leveraging resulting insights to create look-a-like audiences that function as targetable segments for prospecting test and learn campaigns.

The Enrichment Process

First, the deterministic data collected from various touch points across the consumer's journey is pre-processed to understand the linkages between identifiers such as hashed email-id(s), hashed mobile number(s), mobile advertising id(s), IP address(es), and device signature(s), etc. A thorough check for completeness and recency are performed during this stage. These linkages are then analysed using algorithms to form a cluster of unique connections that represent a unique individual without compromising security and privacy.

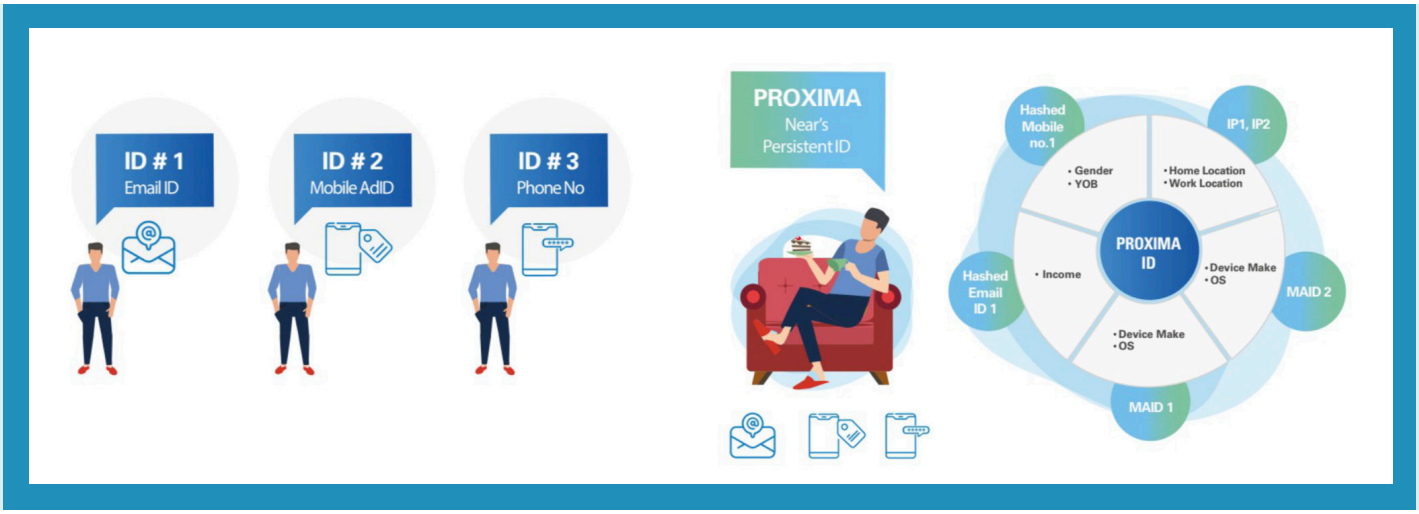
Here, we start with an anchor identifier and then traverse the various linkages from there.

This is done until all the anchor identifiers are exhausted to form clusters of varied shapes and depth. The connectedness of the various identifiers is then calculated and normalised to and the degree of cohesiveness for the clusters. ***The clusters*** are then ranked based on their cohesion and the size, with the larger ones moved down the rank and the more cohesive ones ranked higher. The associations between the different identifiers within the cluster are then scored based on the frequencies with which they are observed.

The clusters with the same identifier in both are then merged to form a larger cluster. Also, the linkages with low associations are removed resulting in the splitting of the clusters. The clusters thus formed are then validated using our patented algorithm that leverages other data sources with a high level of detail to confirm that it corresponds to a unique individual.

The result: A future-proof solution

Going forward, customer engagement across industries will rely on identity resolution methods that are independent of cookies and MAIDs. As an example, Near's PROXIMA identity graph provides this solution for advertisers and marketers across sectors like retail, restaurants and fast-food chains, travel and tourism, and finance.



sourced from Near

Solutions such as this can power data-driven marketing and enrichment offerings through a suite of SaaS products. The users of the platform can leverage audience, spatial, retail, among other data in a privacy-led environment.

Data Clean Rooms

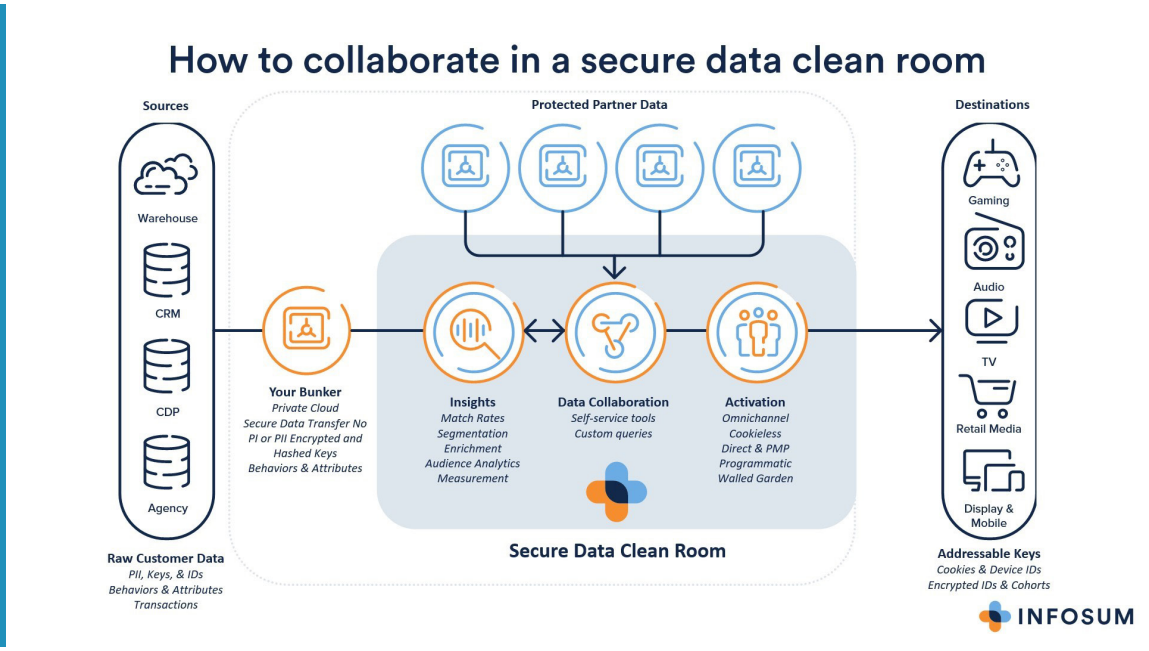
With increased regulation and the deprecation of traditional identifiers used for advertising, brands and media owners need new ways to increase the effectiveness of their data-driven strategies without having to share or expose their proprietary data.

Enter data clean rooms.

Data clean rooms are a safe environment where multiple datasets can be brought together for various marketing use cases, including analysis, enrichment, activation, and measurement. However, traditional data clean rooms risk exposure of customer data by sharing and activating sensitive PII directly with the ecosystem. Many lack the crucial data governance and data security processes necessary to provide a future-proofed solution.

A data clean room provides a secure environment where multiple data sources are matched and analysed, without sharing or compromising the data itself. The safety and security of data combined with the power and intelligence of multi-party computation enable companies to instantly match and analyse data across unlimited datasets in real-time whilst still eliminating the risk of exposure, leakage, or misuse.

Organisations can then look to connect their clean room to other high-quality data partners to maximise the scale, accuracy, and performance of all data-driven strategies including audience planning, activation, and measurement.



Clean rooms are looking to provide a sustainable way forward enabling secure data connections without sacrificing privacy or security. However, it's important to understand that not all data clean rooms are created equal and often don't solve the same needs.

Single-party clean rooms

A Customer Data Platform is an example of a centralised single-party clean room Centralised multi-party clean rooms.

They are great for first-party data management, with centralised data storage & processing, but do not provide growth or scale. CDPs normalise data across first-party customer datasets, create customer profiles based on first-party data and make them available for trigger-based orchestration, usually in a self-serve SaaS platform.

There is, however, no data querying or modelling with external datasets available, no identity resolution or data onboarding and they rely on a singular internal identity graph or ID spine.

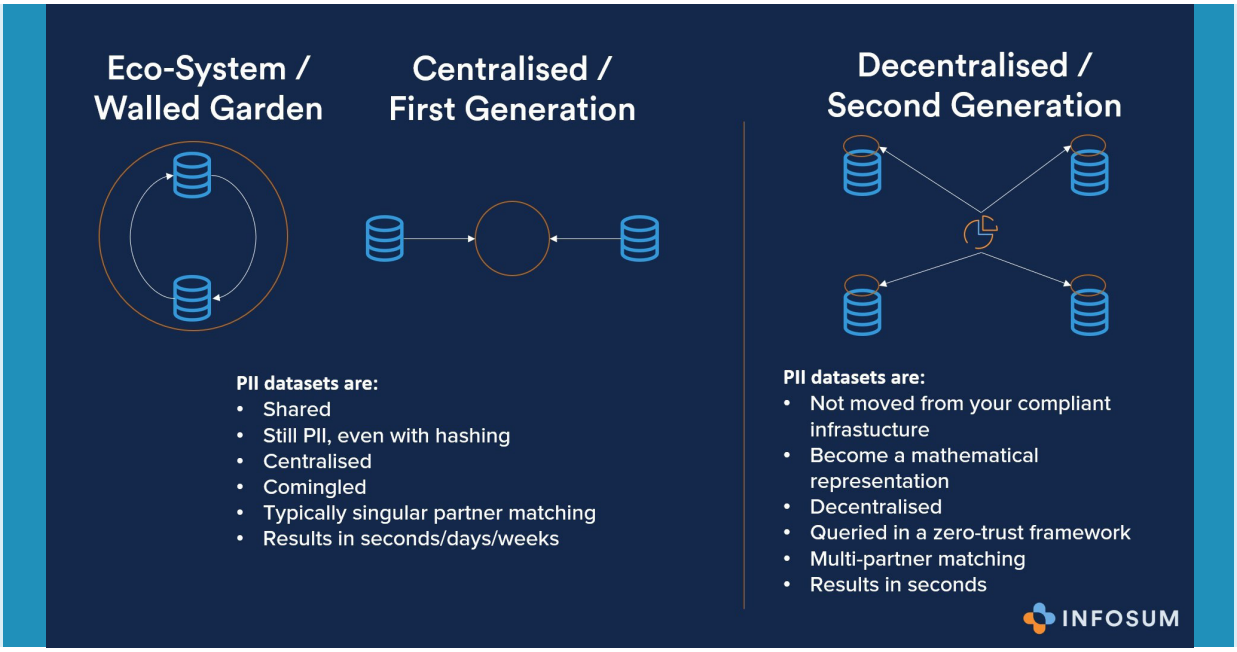
Centralised multi-party clean rooms

Data warehouses are an example of a centralised multi-party clean room that provides the necessary bulk data centralization and management but are complicated to use and are not purpose-built for the protection or privacy of data.

They are used for enterprise data management across first-, secondand third-party data with centralised data storage & processing. Data warehouses normalise data across customer and partner datasets and provide access to structured datasets available for routine analytics and data science.

Data warehouses are usually complex to operate and organise and require costly data science resources to extract insight and value from complex datasets. There is no identity resolution, data onboarding, or segmentation and all collaborating parties must store data within the same cloud system.

The data is also shared directly with other parties for matching and insights, which violates many typical privacy rules around co-mingling and data transfer, under legislations such as GDPR. There are significant risks to be monitored when working across multiple partner datasets, within centralised data clean rooms.



Publisher data clean rooms

Publisher data clean rooms are good for analysis of complex datasets as well as for data science applications, but are not easy to use nor do they provide adequate control or ownership of data. Publisher clean rooms can be used for centralised data storage, analysis, and activation using first-, second- and third- party data but they only provide insights and analysis of their owned and operated properties – cannot be combined or collaborated with any other clean room or dataset.

They usually have limited permissions and access controls that are managed by the publisher and data is kept in a pseudonymized state but not anonymized or encrypted. They really require full trust in the publisher to protect and secure your data.

Decentralised multi-party clean rooms

The truest version of a data clean room, provides an environment that is completely closed off to all parties, including the data clean room facilitator itself, to ensure complete non-movement of data when matching, analysing, and activating.

The primary and most obvious difference between a centralised and decentralised data clean room is how the data from multiple parties is processed. Most multi-party data sharing or data computation solutions require processing to take place in a centralised location, therefore requiring data to move or be shared across multiple systems increasing the risk of exposure leakage, and misuse.

Within a decentralised multi-party clean room the data processing takes place where the data itself is located, eliminating the need for the data itself to move. Instead, a mathematical model of the individuals in each dataset is generated which is anonymous and contains no personal data (PII). It is the mathematical model that moves not the underlying protected data during computation resulting in faster results with greater privacy protection.

All data-driven use cases from identity resolution to personalised customer experiences are unlocked from a single access point to a network of data-rich companies, all while prioritising consumer privacy, and ensuring each company retains 100% control of its data at all times.

This general philosophy of 'zero contamination' has been leveraged from manufacturing and the concept is over 50 years old, invented by Willis Whitfield – who was challenged to find a way to stop microscopic dust particles from infiltrating mechanical components in the manufacture of nuclear weapons. These processes came to revolutionise manufacturing in electronics and pharmaceuticals, improved safety and even enabled further space exploration. That strict approach and mindset should be considered when looking to work in these environments and with these tools. It's privacy-first and zero risk mantra for any businesses, and at all times.

Hence, there are a few simple questions that should always be asked when considering these tools and practices, and ensuring you have the right legal, analytical and technical resources are paramount:
Is there enough scale and quality in the data to justify this solution?

- *Are all the local and global data governance requirements being met?*
- *Is all the data being responsibly and transparently collected and managed?*
- *Will you be able to view individual customer journeys across all devices and offline touch-points?*
- *Can you meaningfully analyse, activate and measure any channel or media partner with full performance transparency – again down to the individual level?*
- *Do you have complete confidence and trust in the vendor and other parties involved in their related practices in terms of responsible data governance?*

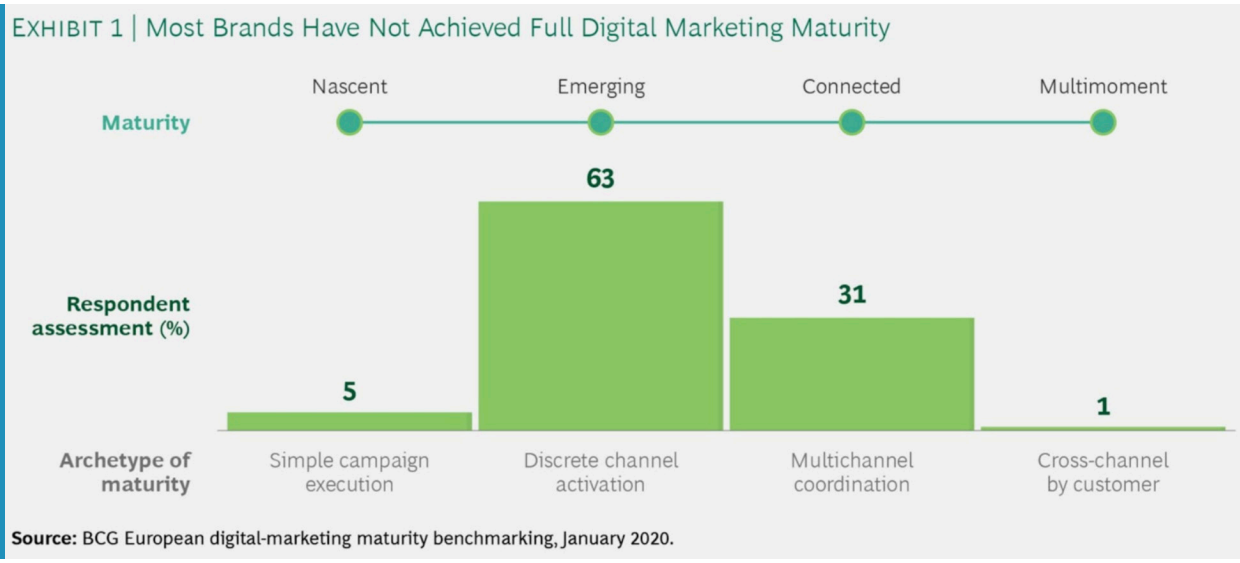
The hope is that with the evolution of clean rooms the industry can start to make effective yet responsible first-party data sharing practices much easier, more efficient and less risky. Our Data council will be keeping on top of this subject and providing further guidance as this product space evolves.

Execution & Usage

Section 6

Using first-party data can help you better understand your customers' needs and deliver a *better customer experience, which can lead to increased performance.*

According to a 2020 study by BCG, companies that link all of their first-party data sources can generate double the incremental revenue from a single ad placement, communication, or outreach. They can also see 1.5x improvement in cost efficiency over companies with limited data integration and still see plenty of opportunity for first-party data to better enable marketing departments across a range of business types.

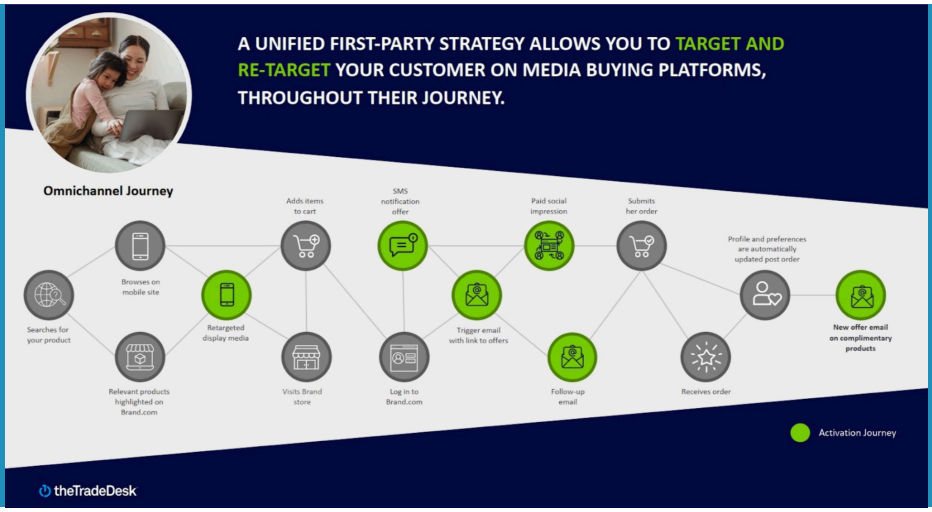


First-party data also provides the foundation for machine learning, helping to predict outcomes and engage with audiences. Companies such as Google are actively investing in first-party data as a stronger foundation for the future, and helping privacy-focused marketers & publishers to do more with their first-party data by making it easier to use, organise and derive insights from trusted, known customer relationships.

Rely on first-party data to engage audiences When you analyze your first-party data for insights, you can better connect with your audience by delivering more meaningful experiences in a privacy-safe way. For instance, you can use first-party data to engage with your best customers. When people share their contact information with your business, you can use Customer Match to reach those same users again as they're moving across Google properties, including Search, the Shopping tab, Gmail, Discovery, and YouTube.

Once you've established a privacy-safe measurement foundation, use Smart Bidding to take action on this data. Smart Bidding strategies use machine learning to optimize for conversions or conversion value in each and every auction. And, because for many businesses, some conversions are worth more than others, a value-based bidding strategy, such as Maximize conversion value with an optional target ROAS, can help you optimize for total value, rather than volume, by automatically adjusting your bids to reach your highest-value customers.

Value-based bidding, a subset of Smart Bidding, works across different marketing objectives. If you are already bidding towards value, you can consider more advanced strategies using your first-party data, such as bidding towards profit or expected lifetime value. Google's machine learning will work with the inputs you set to get you closer to meeting your business outcomes. [Source]



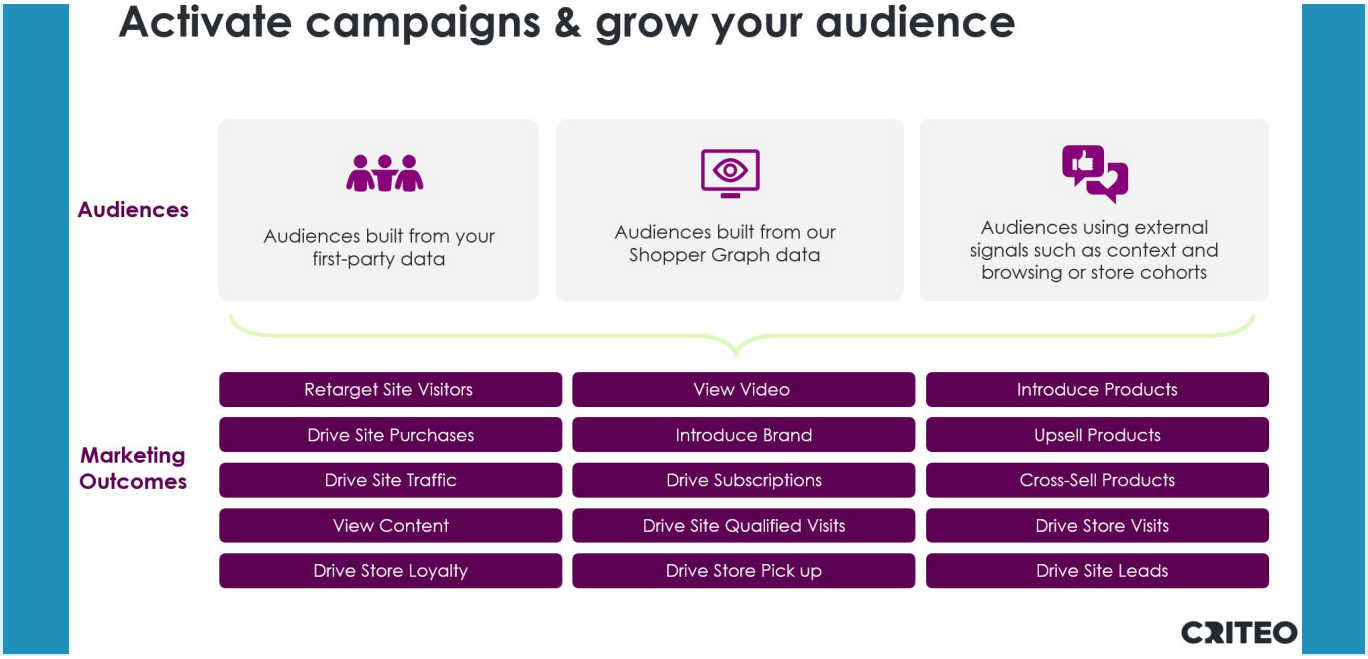
Publishers have turned to first-party data for a variety of reasons, including the industry-wide uncertainty over the future of attribution. In the absence of any consensus replacement for the third-party cookie, using first-party data to identify users solves the problem of attribution, but only for logged-in visitors.

For most publishers, the size of their logged-in audience pales in comparison to the size of their fly-by visitors, which formerly they could identify using third-party cookies. As a result, while publishers regard their first-party efforts as a viable way of understanding their most-engaged visitors, marketers are concerned about the challenge of scaling this offering, according to an industry source with knowledge of the matter.

"Some publishers are experimenting with registration walls as a means of solving the problem, but the method has its fair share of drawbacks, such as their potential to throttle traffic or disrupt the subscription conversion process," - said Michael Silberman, svp of strategy at subscription management platform Piano.

Publishers' embrace of first-party data also stems from concerns over data leakage and devaluation. By creating a walled garden, publishers can ensure that marketers must come to them to access insights about their audience. However, in their efforts to protect user data, publishers can limit brands' ability to cross-reference their first-party data against the insights they collect. These precautions protect user data from leakage, but they do so at the expense of heightened targeting.

This limitation, one simmering throughout the marketing ecosystem, remains to be substantially addressed. Clean rooms, which allow parties to commingle hashed data in a privacy-compliant manner, offer one potential solution, but––like registration walls––the concept is relatively new and few parties are eager to volunteer their bottom line for experimentation.



Project Rearc & IAB Tech Lab's Seller Defined Audiences (SDAs)

Since IAB Tech Lab announced Project Research and released four initial sets of specs in response to the deprecation and/or limitation of third-party cookies and other identifiers, there has been a lot of collaborative work in the background.
These specifications have drawn a clearer focus on how one of the (three) future-proof approaches will be the use of identity service to competently link 1:1 audiences between publishers and advertisers.

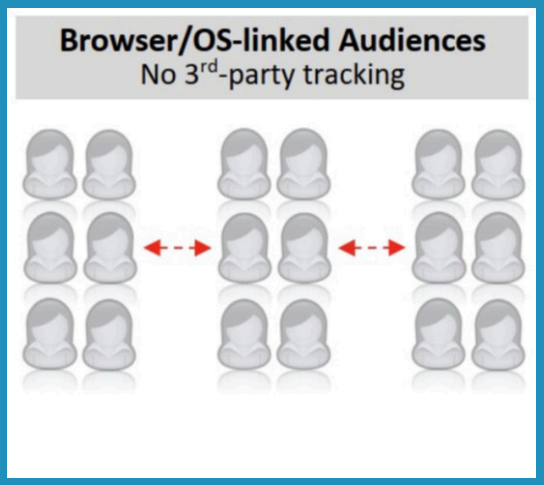
These services will require either an explicitly opted-in device-based ID or secure, user-enabled ID from a login, email, etc. potentially connected to a clean room approach.

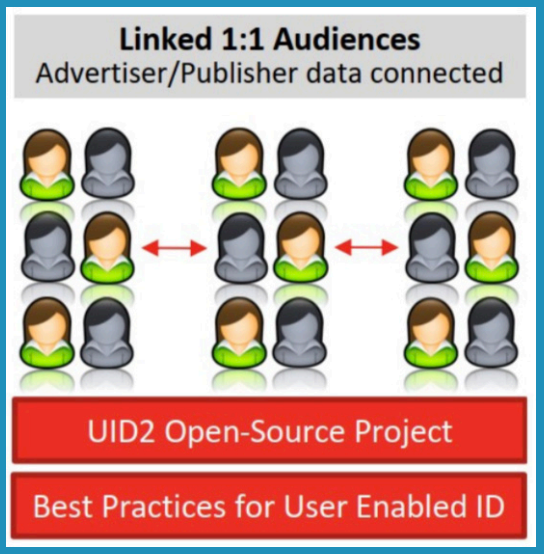
They will also have to be secured, have highly transparent uses, and offer consumers a full suite of privacy-focused controls.

As a key element of 'unliked 1st party audiences' is the release in early 2022 of the Seller-Defined Audiences specs as a significant step in enabling publishers, DMPs and data providers to scale first-party data responsibly and reliably without the risk of leakage or reliance on technologies that will ultimately be limited (e.g. 3rd party cookies, IDFA & GAID).

Structured, publisher-defined audiences are an inherently-consented, easy and trustworthy way to bring these signals to life without requiring any exchange of user identifiers in the process. These privacy-by-design specifications enable both contextual signals and audience segments (across demographics, interest, and purchase intent attributes) to be safely defined, labelled, scaled and monetised by leveraging anonymous taxonomy IDs in place of cookies and mobile IDs.

Programmatic buyers can then differentiate these audiences and access those they desire within bid requests, through referencing existing data labelling and transparency standards. This will enable buyers and sellers to seamlessly transact, using valuable consumer insights, and without fear of data leakage and loss of scale, and whilst meaningfully addressing privacy considerations in the changing landscape.





In terms of the core benefits it's worthwhile highlighting *these for clarity:*

Privacy safe future-proof solution :
as publishers & data providers will not have to share user identifiers with external platforms and companies to activate first-party data for buyers.

More efficient process:
as SDA removes the need for any manual deal-ID creation processes and can be executed more efficiently similar to PMPs.

Flexibility and compliance:
custom taxonomies can be supported, but only through following consistent standards and aligning to industry-led non-profit compliance processes.

Works across all environments :
from browsers and in-app to OOH and CTV.

Protects premium audiences:
as publishers can share segments with buyers without revealing any first-party data IDs, minimising any risk of leakage.

No user-IDs required:
SDAs are unique as an approach as no exchange of user identifiers between publishers, SSPs, DSPs and DMPs/CDPs are required. Publishers curate their audiences into standardised demographic, interest, and/or behavioural audience cohorts that can be passed into bid requests to any DSPs bidding on their inventory.

The process leverages IAB Tech Lab standards that are already in place (IAB Tech Lab's Audience Taxonomy, Data Transparency Standard & Transparency Center) and have recently been upgraded toenable the workflows for the SDA specs.

Ultimately the process will look something like:

1. Collect and curate audience segments

Publishers can determine audience attributes based on customer interactions on their properties using the IAB Tech Lab's Audience Taxonomy. This describes and labels segmented audiences across some 1,600 demographic, interest, and purchase intent attributes.

2. Map and label targeting attributes

By leveraging the IAB Tech Lab's Data Transparency Standard publishers can provide simple taxonomy descriptions and data transparency disclosures to buyers through 20 different fields that must be populated for each segment ID to provide more information about each segment.

As this process involves self-attestment the IAB Tech Lab have also developed an associated compliance program for this standard that allows providers to demonstrate the quality of their labelling via a Tech Lab 'seal of approval' issued upon program completion. This can provide buyers the assurance that the information within each 'Data Label' is not being misrepresented by the seller.

3. Share SDAs with Buyers in real time

Thereafter Publishers can relay the resulting anonymized taxonomy IDs within an OpenRTB bid request to inform downstream signalling by buyers – using the existing user, data, and segment objects from the ORTB 2.6 specification.

Provider Name:

The unique domain of the entity making the attribute /cohort determination

Segment ID (s):

The provider's declaration of the ID(s) that best describe its internal segmentation

Taxonomy Name:

The taxonomy range in which the Segment IDs / values can be found

4. DSPs review and decision against segment IDs

Buyers interested in bidding on an SDA can review the relevant segment IDs in real-time to fully understand and evaluate the cohort before bidding. The IAB Tech Lab's Transparency Center provides a centralised location and UI to search and discover DTS metadata before making any purchase decision.

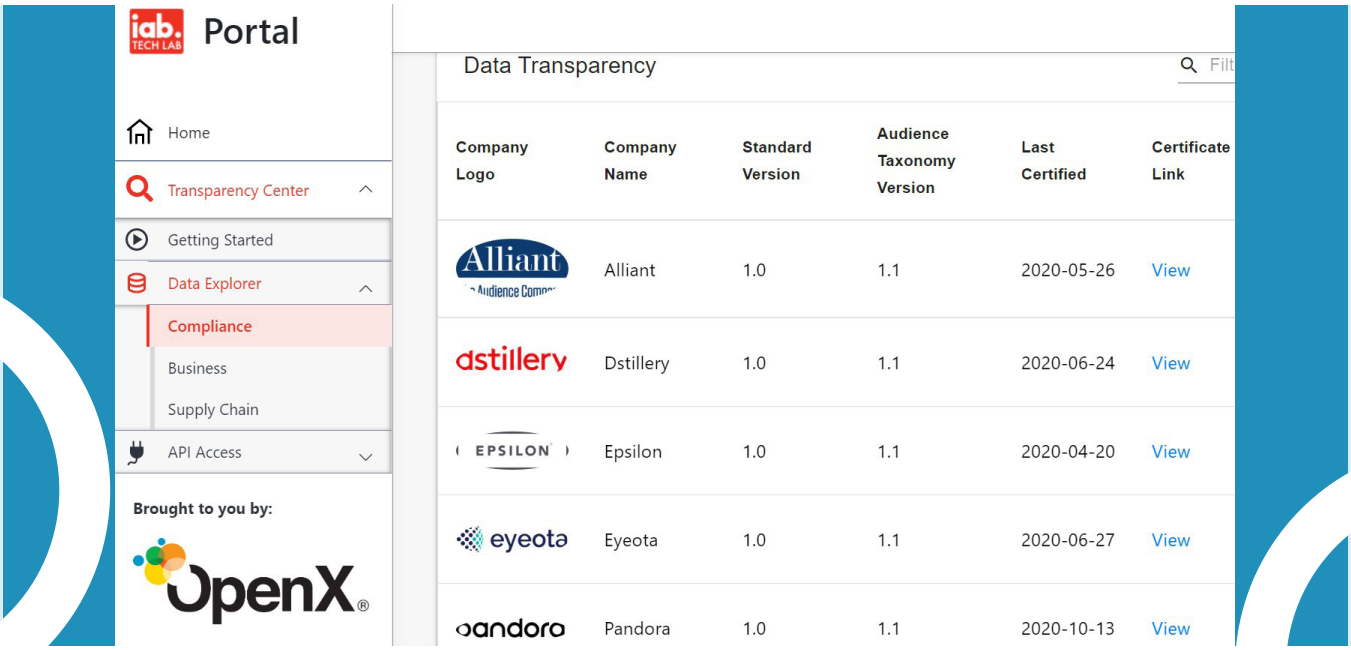
It also allows for Transparency Center subscribers to retrieve the metadata via an API and once a DSP has verified the data, it can then store the SDA mapping in their system and make the SDA segment names available for targeting by buyers within their UI. DSPs can then match incoming bid requests that contain SDA segment IDs with SDA segment names that their clients target on their campaigns.

By leveraging these already-adopted specifications in new ways, SDA establishes that publishers or their data partners:

1) determine audience attributes based on customer interactions on their properties,

2) map those attributes to standardised taxonomy descriptions and data transparency disclosures

3) relay those anonymized taxonomy IDs within OpenRTB to inform downstream signalling by buyers.



Company Logo	Company Name	Standard Version	Audience Taxonomy Version	Last Certified	Certificate Link
Alliant	Alliant	1.0	1.1	2020-05-26	View
dstillery	Dstillery	1.0	1.1	2020-06-24	View
EPSILON	Epsilon	1.0	1.1	2020-04-20	View
eyeota	Eyeota	1.0	1.1	2020-06-27	View
pandora	Pandora	1.0	1.1	2020-10-13	View

The IAB Tech Lab has leveraged Prebid as a turnkey solution to pass data into the bid stream.

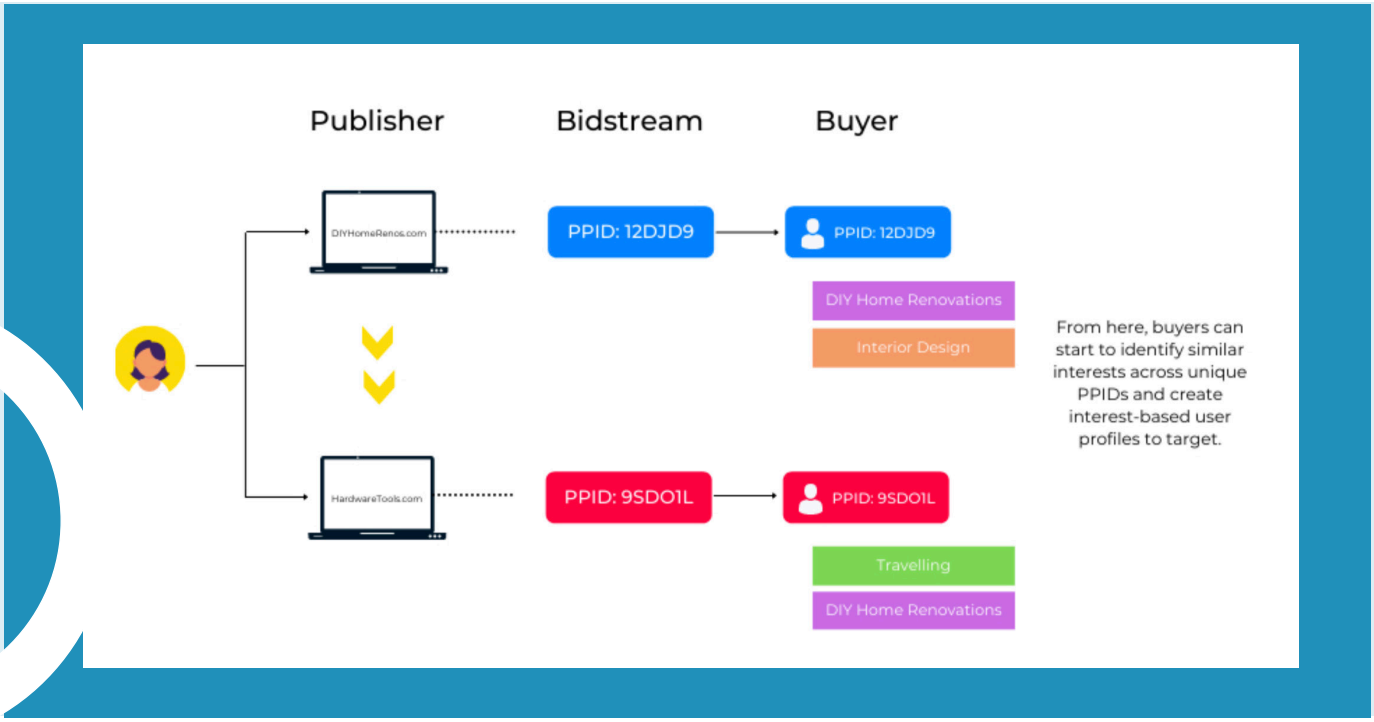
This is not a prerequisite but using the bespoke integration with prebid. Js is much easier for users of this free and open source suite.

To also enable vendor specific taxonomies a new extension has been developed called segtax, which stands for 'Segment Taxonomies' and can identify a specific taxonomy used to determine the provided segments. This model supports using taxonomies other than IAB taxonomies, but all taxonomies must be registered with the IAB Tech Lab in order to be assigned a dedicated integer.

For publishers, it is important to get involved in relevant forums, engage in testing and any relevant discussions and have their data in the correct format to enable these new fields to sit alongside their current data product. Advertisers should also engage with tech vendors on the required processes to enable their ad buying needs, test as soon as possible with partners and look to develop resulting innovative strategies.

One existing solution that is already in place and is conceptually a similar approach is Google's publisher-provided identifier (PPID) feature in Ad Manager 360. For current clients of this platform experimenting with PPIDs as a starting point is potentially useful as the approach is somewhat aligned, albeit not exactly the same and not aimed at fully enabling the open internet in the same manner as SDAs. The PPID is a string of alphanumeric figures assigned to each individual user when they visit the website.

This enables publishers to attribute all their activity to a single profile, segment these users based on their interests and add PPIDs into groups defined by common interests. These values are then passed into GAM360 to accurately distinguish users within its ad audience – even when cookies have been disabled.



Commercial Examples & Case-Studies

Section 7

The WSJ in Partnership with Google Ad Manager Case Study

Advertisers were 37% more likely to renew if their prior campaigns used first-party data

The Wall Street Journal welcomes its cookieless future, and advertisers have taken notice.

The Journal has reoriented much of its advertising business in recent years to collect and utilise first-party data, including standing up proprietary software like Thematic, Safesuite and Insite. It also has access to a wealth of first-party data, given that its parent company, Dow Jones, has more than 3 million digital subscribers across its properties.

Google approached the publisher to propose the case study, as The Journal wanted to see how its first-party data efforts affected client retention, Minkin said. The companies also have a long working history on Google Ad Manager.

The efforts of The Journal to improve its first-party data reflect the larger, identity-based efforts transforming the industry. As the deprecation of the third-party cookie within Chrome grows closer, and the marketing ecosystem remains split over its replacement, publishers have embraced first-party data as a failsafe means to identify and transact against their audiences.

"Seventy-two percent of our audience segments are built or informed by first-party data," Minkin said. "So we're going to be well positioned to be entirely off third-party data long before Google kills that cookie."

How The Exchange uses its first-party data

WSJ|BG, the in-house advertising department serving The Journal and Barron's, uses its wealth of first-party data and suite of proprietary tools to create audience segments that it can sell to advertisers. It creates attribution-based segments using subscriber information and contextual segments based on reader behaviour.

More than 70% of the audience segments that The Journal sells are built or informed by first-party data, according to the case study. From July to December 2021, audience targeting generated 21% of first-party advertising revenue, while content targeting generated 71%.

Once it has created these segments, WSJ|BG markets them to clients via direct and private marketplace deals on Google Ad Manager. To streamline direct deals, WSJ|BG makes all available segments visible in their order management study, according to the case study. Once a data-driven deal is struck, many of the first-party segments are pushed to Ad Manager using Publisher Provided Identifiers, where the ad ops team traffics the ads and pushes them live.

Content taken from AdWeek:
https://www.adweek.com/media/the-wall-street-journal-first-party-data-key-to-repeat-media-buys/
To read more on this case study visit:
https://admanager.google.com/home/resources/wsj-bg-first-party-data-performance/

Suncorp unlocks Business value through leveraging 1st party data across portfolio of Brands.

1st Party Data Opportunity

Through onboarding a Customer Data Platform (CDP), 1st party data infrastructure was aligned across Suncorp's portfolio of brands unlocking the opportunity for new capabilities. As part of this project, it was identified that merging Suncorp's 1st party data alongside an ecosystem of complimenting data partners would:

Increased addressability of channels to enable personalisation, advance customer understanding by enriching 1st party data segmentation, and provide new analytics capability to better measure media performance outcomes.

The following case studies highlight examples of how Suncorp brought to life advanced customer understanding through the enrichment of 1st party data, along with the personalisation opportunities this represented.

Bringing this to life

Leveraging Customer Journey Insights

AAMI embarked on a strategic data partnership with a major automotive marketplace, merging data sets with the ambition to deliver more personalised experiences.

As a result of this merged dataset, AAMI was able to understand audience pains and gains throughout the car buying journey. Through activating their own customer data within this, they were able to then surface the right optional extra based on what was known about the customer and their journey.

This data-led personalised approach is delivering significant double digit ROI uplifts.

Leveraging 1st party to demonstrate media sponsorship value

Leveraging a data partnership with a major Australian broadcaster, Suncorp were able to demonstrate the Business impact delivered from a significant content sponsorship. In matching their 1st party data with the broadcaster, they were able to isolate those customers (and non-customers) who had been exposed to Suncorp messaging throughout the broadcast.

Based on this customer exposure analysis it was determined that the sponsorship drove a significant increase in average product holdings and nearly 2,000 additional policies.

Improving acquisition outcomes through suppression

Leveraging a data partnership with a major Australian broadcaster, Apia were able to exclude existing customers to drive greater efficiencies from new customer exposures. Apia matched their 1st party data with the broadcaster which allowed them to identify existing customers.

These customers were excluded from the audience targeting approach allowing for more personalised, acquisition focussed messages to be surfaced to potential customers whilst watching their favourite content. This revised targeting approach delivered nearly double digital efficiencies in media and via the broadcaster partnership, established a runway for a variety of future, data-led initiatives that could help combat challenges in potential privacy regulation updates.

RETAIL AND XPON

This retail group sought to deliver personalised marketing journeys across multiple online and offline channels at scale.

Due to a changing privacy landscape, the organisation needed to drive the uptake of new processes and technologies to alter how customer data was collected, connected and leveraged across the organisation.

Check out how XPON delivered on their KPI's.

PETCARE BRAND AND BLIS

A leading petcare brand wanted to better understand its target audience and increase store visits over the Christmas period.

Blis ingested the client's first party data into its platform, further enriching it with Blis' first party location data, telco data and IRI petcare sales data in order to reach and prospect new customers that own pets and have a high propensity to purchase petcare products.

See how Blis delivered on their KPIs

COCO VILLAGE AND THE TRADE DESK

Learn how high-end children's furniture and toymaker, Coco Village is using their first-party data effectively for global expansion and reaching new potential customers.

VODAFONE AND ADFORM

How Do First-Party IDs Compare to Third-Party Cookies? Vodafone CZ and Czech Publisher Exchange (CPEx) Discover Incredible Results.

ICARE AND PUREPROFILE

Pureprofile were tasked to cement icare's position as the best choice for soft, sustainable toilet paper.

Check out their solution!

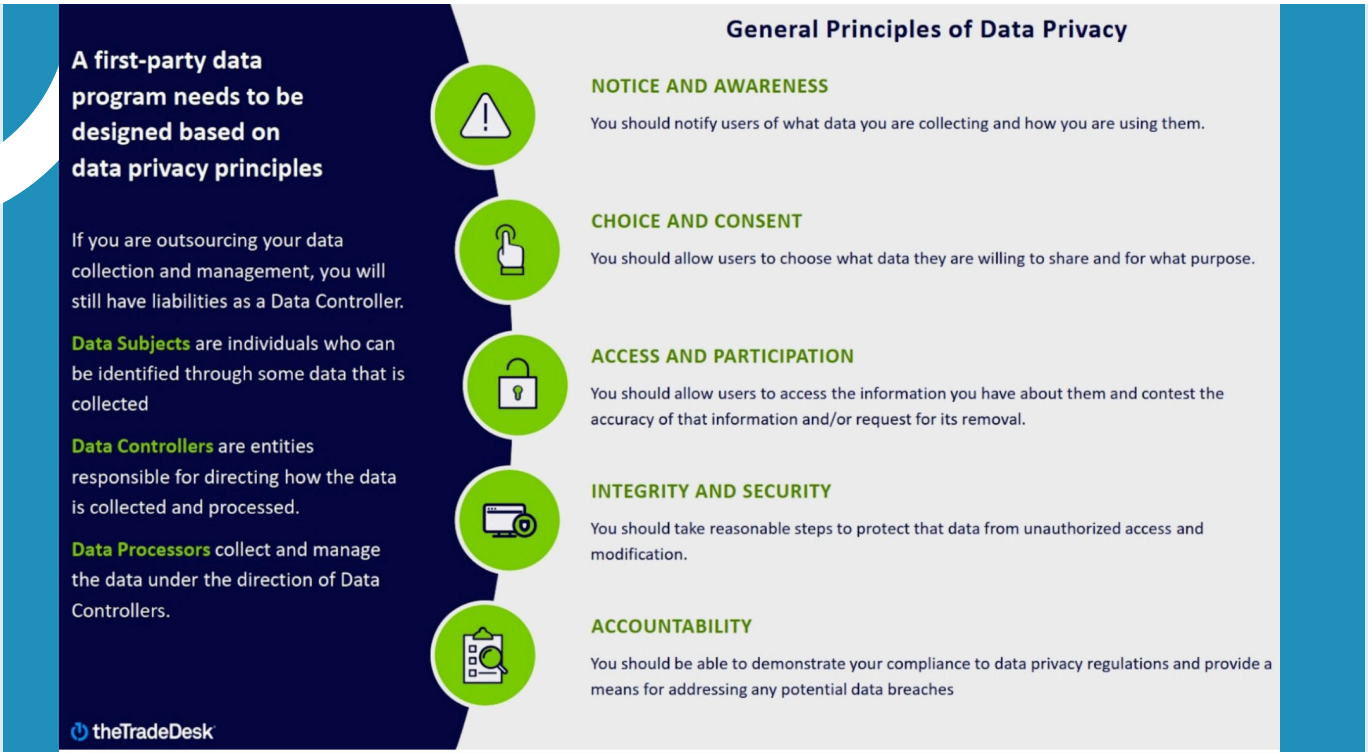
CARSALES AND CIVIC DATA

Carsales wished to move beyond simple CDP / 1PD data management. With increased regulations and growing device/browser limitations; a need to flexibly activate and control data compliantly across existing and future ecosystems was required. Check out how Civic Data worked with Carsales to achieve this.

Consumer Consent & Privacy

Section 8

Building a direct relationship with customers based on responsibly-gathered first-party data can be an effective way to drive consumer trust with your brand.



Please note, these General Principles are a guide only. The terms "Data Controller" and "Data Processor" are terms used under GDPR rather than the Australian Privacy Act.

Privacy Reviews – Looking ahead & potential future legal changes

The Australian federal Attorney-General's department is currently reviewing the Privacy Act 1988. While it is unclear at this stage what changes will actually go ahead, the Discussion Paper sets out a range of potential reforms intended to strengthen privacy protection for consumers in the evolving online environment. These include:

Amending the definition of 'personal information' and clarifying the types of information capable of falling within the new definition. New obligation which shift the responsibility of privacy compliance from consumers to organisations. Increased options for consumer choice and control – for example, through pro-privacy requirements or default settings.

Significantly increased maximum penalties to bring the penalties for breaches of privacy more in-line with competition and consumer law remedies. Additional obligations for certain large online platforms, for example, social media platforms, for example with respect to children and vulnerable consumers.

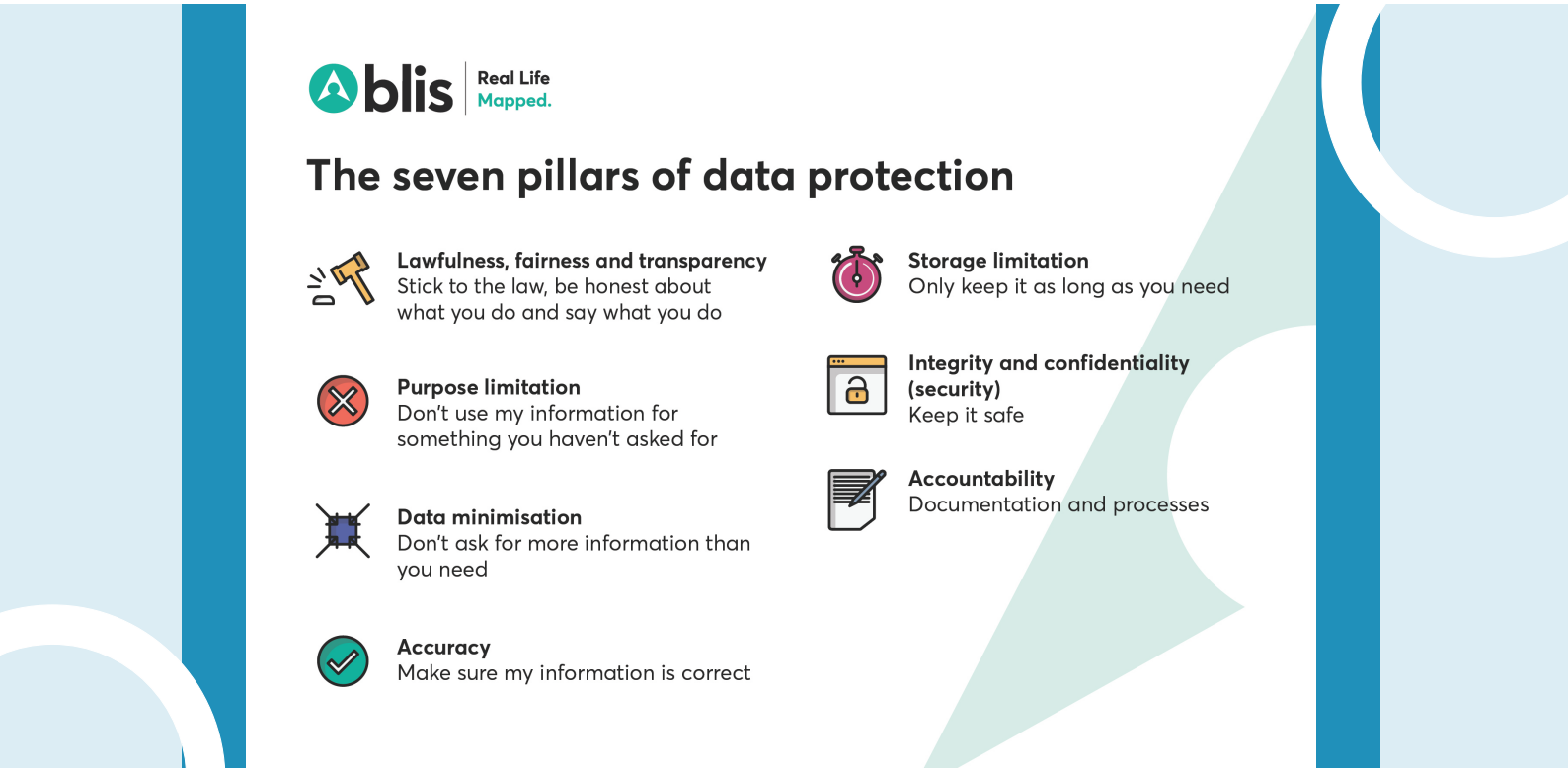
Please note, these proposals are only proposals at this stage. We will know more about the new Government's commitments on privacy by the end of 2022. To review the IAB Australia submissons click here.

Consumers are demanding more privacy, but they are not saying don't advertise to me. They simply want more respect for their data.

For their data to be treated confidentially and respectfully, not to be harvested without their permission, not to be used for ill purposes and not to be shared unexpectedly.

This consumer desire has led to governments around the world to look to the GDPR for inspiration and update their own privacy regulations including USA states such as California and Colorado, New Zealand, Brazil and South Africa. Whilst the nuances of each privacy regulation will be different and logistically that does bring challenges to any global organisation, at its core, all data protection regulations include these pillars:

- **Lawfulness, fairness and transparency: Stick to the law, be honest about what you do and say what you do**
- **Purpose limitation: Don't use my information for something you haven't asked for**
- **Data minimisation: Don't ask for more information than you need**
- **Accuracy: Make sure my information is correct**
- **Storage limitation: Only keep it as long as you need**
- **Integrity and confidentiality (security): Keep it safe**
- **Accountability: Documentation and processes**

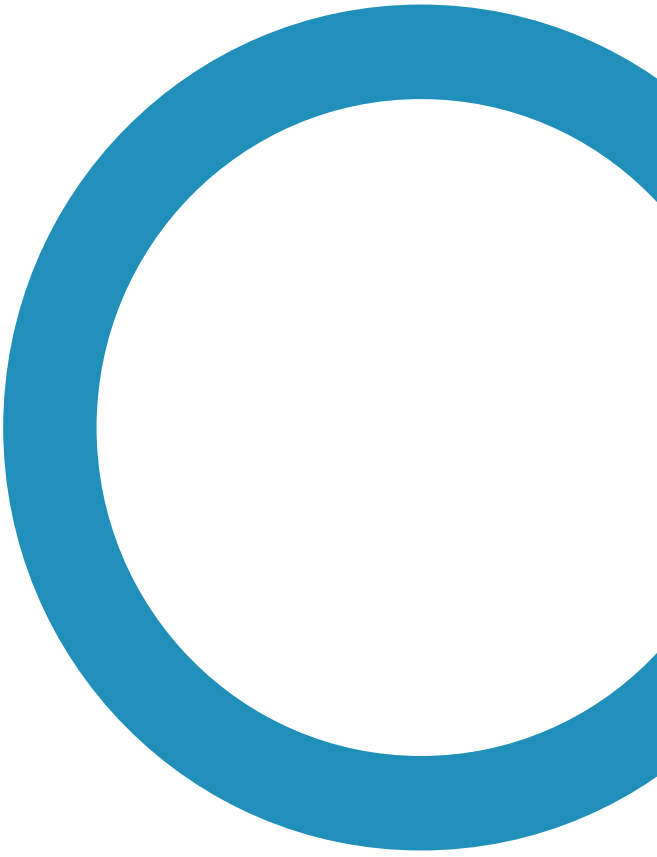


As Australia starts to reform and modernise the 1988 Privacy Act, how can businesses prepare for the uncertainty?

To answer this we would suggest a few ideas building on data protection principles we have just shared:

- **When building new advertising products for first-party data, think about how they would work in a privacy-first world.**
- **When structuring your organisation, think 'how can I ensure each member of staff will take accountability for the privacy and security of the personal data that flows through our systems?'**
- **When bringing on board new partners and vendors, look at their track record in terms of cybersecurity and privacy – think** *'would I trust them with my personal data?'*

We don't know what the reform will look like, but we know it is coming. Our recommendation is that rather than debating its exact architecture, such as what will be classified as personal data and opt in vs opt out, just start preparing and changing, as it will make the transition so much easier.



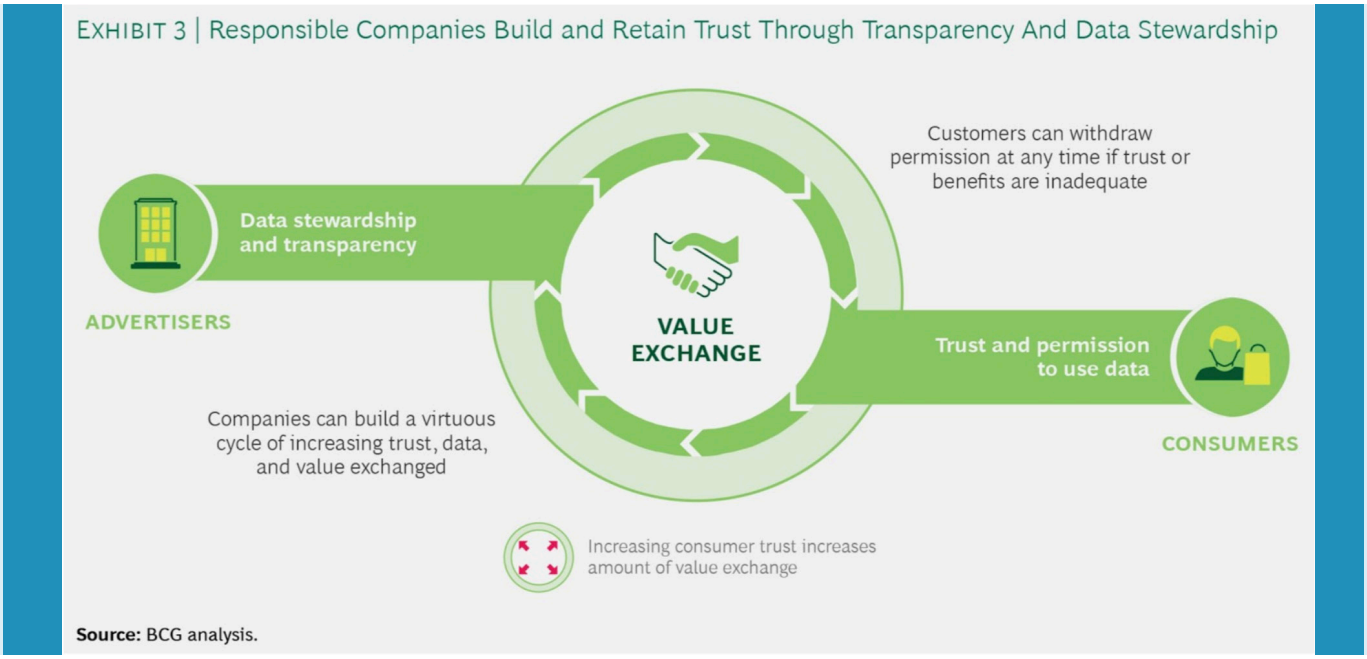
The Consumer 'Value Exchange'

Section 9

The consumer value exchange is the value the consumer will receive in return for providing their personal data.

Having a consumer submit a lead or sign up and log into the site each visit will give the marketer a rich understanding of who their customer is, but in turn, the brand needs to consider what the consumer will receive for sharing their data.

For example, a logged in interface the consumer may receive additional information such as historical purchase information, discounts or express delivery.



When a marketer sets ups their 1st party data strategy correctly through leveraging the relevant tagging and collection methodology, this paves the way for advanced marketing strategies such as:

- **optimal marketing strategy through Recency Frequency Monetary (RFM) modelling**
- **consumer's likelihood to convert on site (Propensity Modelling).**
- **segment audiences based on their value to the business, and apply relevant marketing plans (e.g. search optimisation, retargeting, suppression etc.)**
- **customer lifetime value and journey.**

The insights afford marketers to deliver more relevant messaging, at a more suitable cadence to the consumer. Similarly, marketers can also choose to negatively target or suppress their marketing towards consumers who have a very low receptivity to the brand.

In October 2021, Ipsos released a local report called 'Digital Data Exchange: The Consumer View', in which it found that 87% of Australians declared that they were supportive of online content and service providers making their money from advertising where access to content remains free for consumers.

This report provided the Australian industry with some robust local data to quantify the understanding that Australians have in relation to both the funding of their digital media and services as well as the data value exchange. The importance of transparency and control were key themes, with 81% of consumers stating they want 'more control and choice' over the collection and use of their personal information, and 46% stating they wanted companies to stop sharing their information with third parties without consent as a high priority.

Also noted was that the most important levers for making consumers more comfortable about sharing their data included being more upfront with how the data collected will be used (47%) and collecting only the data that is needed (46%). Unsurprisingly, consumers were also more comfortable sharing their data with brands they trust.

The key findings of the report included:

- 35% of people said they (at least sometimes) choose not to deal with an organisation because of concerns regarding privacy.

- Transparency on what data is collected and how it is used is the key driver to a high level of trust in providing personal information (43%), however sound corporate values (such as having a good corporate reputation, 40% and being ethical 39%) are nearly equally key trust drivers.

- Trust is top of mind when consumers are faced with consent notices. When presented with pop-up messages on websites and apps about that content provider using cookies or other tracking techniques and requesting consent to track their activity, 63% of consumers are evaluating these before deciding to accept or not, trust in the brand is a major factor in their considerations.

- 38% feel comfortable sharing their purchase history with a brand online if requested, 34% feel comfortable sharing browsing history and 38% personal details such as email, phone, or address.

- While nearly all Australians think privacy of their information is important when choosing digital content and services only 3 in 10 people feel their understanding of data protection and privacy rights is of a high standard.

- Ultimately 8 in 10 people want more control and choice over the collection of their personal information, while 69% care about their data privacy but don't know what to do about it.

- However, 70% of respondents also indicated they were unaware of how online content providers make their money.

Download the full report **here**

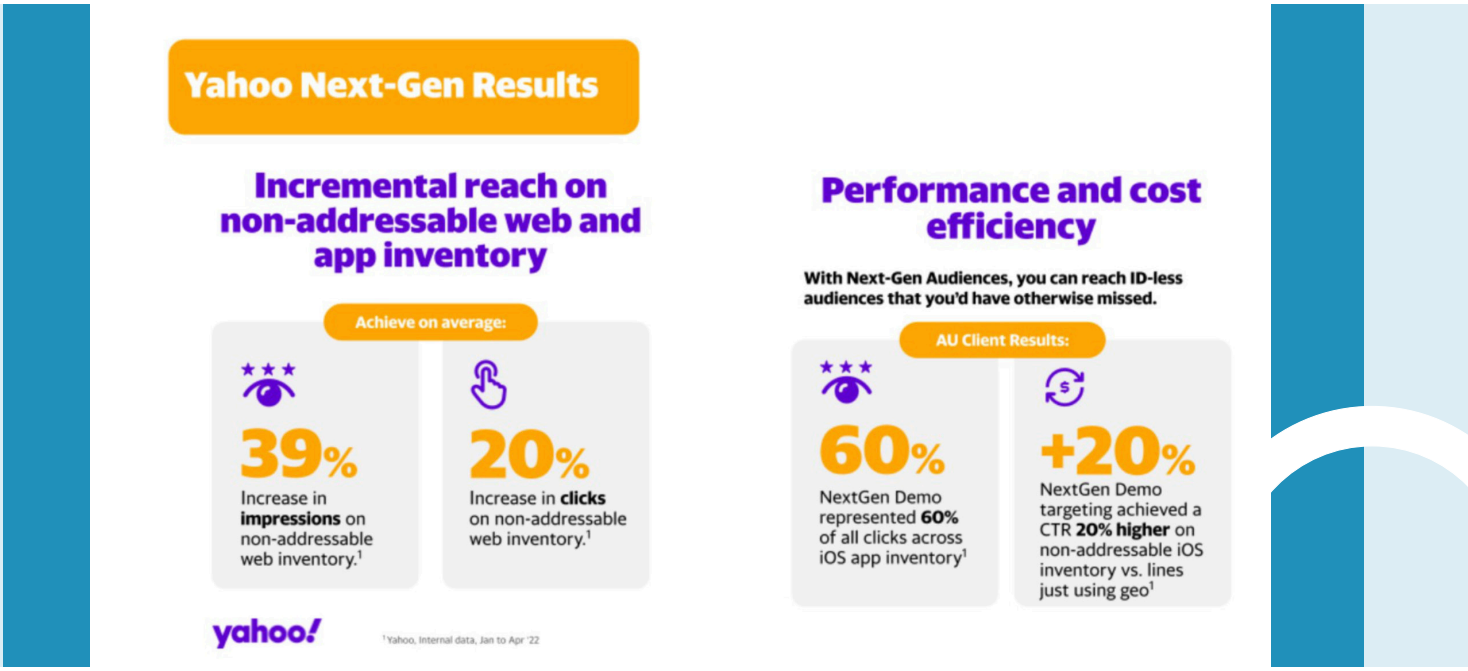
Future developments in this area

Section 10

With new regulations and changing privacy laws put in place across the globe, depreciation of third-party cookies, and Apple's privacy updates on iOS14, there has been a significant decrease in addressable inventory.

An example of how to preserve audience targeting and reach in non-addressable environments is Yahoo's NextGen Audiences.No personal data is stored and it is built to comply with existing and emerging privacy laws across the globe.

- NextGen Audiences are a privacy preserving solution. They work without identity, but instead rely on a sample of first-party data to infer real-time audiences on ID-less traffic.
- NextGen Audiences are currently available across in-app iOS inventory for users who have opted-out from app tracking (apps on iOS 14.5 and above), as well as on web publishers who have adopted ConnectID.
- Next Gen audiences provide results. For a recent AU advertiser, they were able to drive additional clicks across iOS app inventory for their targeted demographic of 25 – 65 year-olds, whilst out performing other tactics.



Thanks to NextGen Demo targeting, this AU home security brand was able to drive additional clicks across iOS app inventory for their targeted demographic of 25 - 65 year olds, whilst outperforming other tactics.

*Flurry ATT opt-in rates - https://www.flurry.com/blog/att-opt-in-rate-monthly-updates/

IAB Tech Lab's ID Transparency Standard

IAB Tech Lab has recently released draft specs to enable yet further transparency to the supply chain by enabling publishers, agencies and brands to declare the identity services they work with. The approach aligns with the other transparency standards, in the .json file being stored at the root domain for easy manual access by humans and readable by machines & crawlers (as you can with ads.txt, sellers.json and buyers.json).

The id-sources.json standard aims to:

- **Provide a standard way for companies to declare which user identity sources they use.**
- **Work like the other supply-chain transparency standards as a participant hosted, structured declaration that machines can read.**
- **Ease ad campaign execution between advertisers, publishers, and their chosen technology providers by making it explicitly clear who supports what.**

By knowing exactly which identifiers are used by which publishers, id-sources.json should help provide greater clarity into ID adoption. Brands and agencies could map out which publishers work with which identifiers and match these against their own audiences, which will themselves be associated with different identifiers. This will help them figure out where in the publishing landscape they can locate their addressable audiences.

For the full set of specifications simply visit:

https://iabtechlab.com/wp-content/uploads/2021/10/id-sources_pc-2021-10.pdf

IAB Data Label Overview

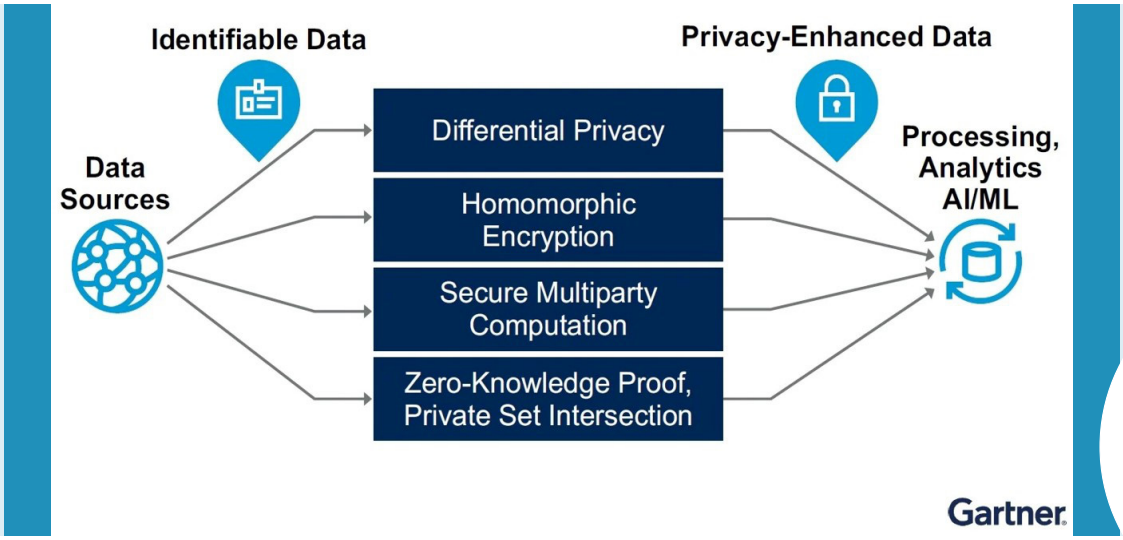
IAB's Data Transparency Label is intended to give every marketer, agency, data provider and publisher a clear view of the audience segments they use.

This is a global initiative set out by **IAB Tech Lab** and it's **Data Transparency Standard Compliance Program** to bring transparency standards to the data marketplace.

Privacy Enhancing Technologies

Privacy Enhancing Technologies (PETs) are a category of technologies that enable, enhance and preserve the privacy of data throughout its lifecycle, including when being shared with third-parties. These have been quietly at work in sectors such as finance and health for some time, but have recently been attracting more interest as more industries (including online advertising) grapple with the increased capabilities of technology whilst also managing the requirements of tighter legislative scrutiny and obligations of increased regulations.

In Gartner's recent Top Strategic Technology Trends for 2022 report, privacy-enhancing computation was highlighted (see image below) as a key trend enabling secure data processing, sharing, cross-border transfers and analytics, even in untrusted environments.



Traditional examples of PETs include secure multiparty computation, homomorphic encryption and differential privacy.

Differential privacy:

Enables access to data containing consumer personal information without revealing the identities of the individuals, thereby ensuring confidentiality.

Homomorphic encryption:

Is a method of encryption that allows computations to be performed on encrypted data without first decrypting it with a secret key. The results of the computations also remain encrypted and can only be decrypted by the owner of the private key.

Secure multiparty computation:

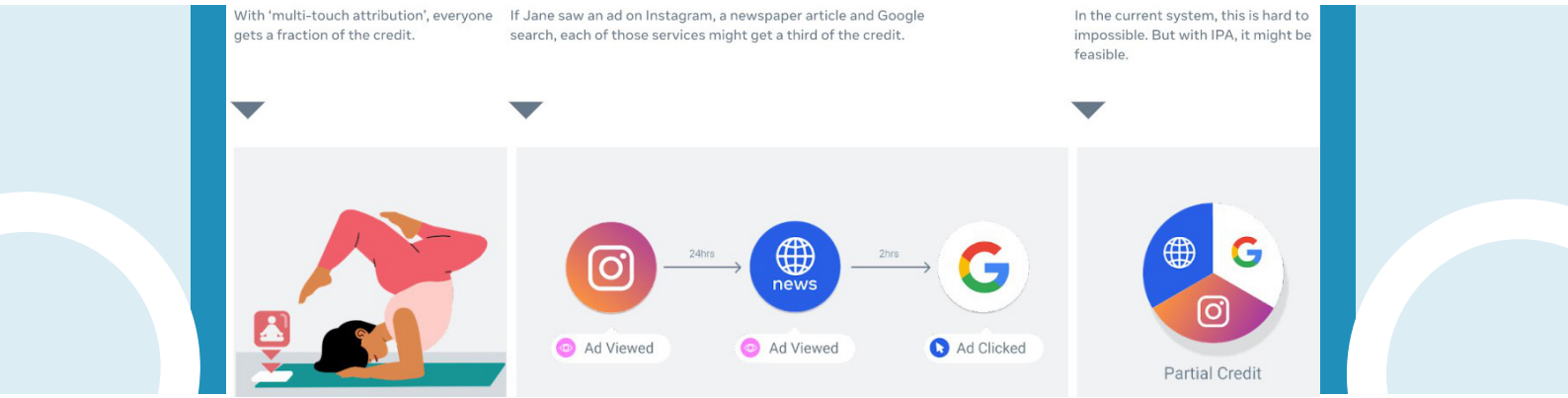
This enables data scientists and analysts to compliantly, securely, and privately compute on distributed data without ever exposing or moving it. PETs can enable trusted, decentralised collaboration by allowing participants to securely cross-match or analyse disparate data holdings and extract value without the risk of exposing any sensitive information.

Companies keen to leverage data they don't own or control are increasingly attractive as collecting, managing, and maintaining large first-party data holdings is difficult, expensive and risky. Second and third-party data sources can provide enormous value, but can also increase risks – and PETs can preserve the interests of the various contributors whilst also expanding usability for the data owner since these protections can help overcome any legal or risk objections.

Meta (Facebook) have for some time now been running a number of PETs initiatives – including On-Device Learning, whereby a consumer's phone would play the key role in determining whether an ad matches their preferences without the need for an ID being associated with the process. For more information on this project click here

These solutions enable businesses with legitimate access to large amounts of first-party data to safely and securely keep and update that information without directly accessing the raw data, negating the risk of ever exposing the consumer data. Thereafter, other companies (second parties) can bring their own data and campaign insights from one clean room and compare it with another, again without directly exposing customer data.

Meta have also been working recently with Mozilla on a project called Interoperable Private Attribution. This is a proposed interoperable system for cross-platform attribution that would enable accurate ad measurement whilst still ensuring user privacy through Secure Multiparty Computation.



To read more on the Interoperable Private Attribution initiative simply click here

Global Privacy Platform (GPP)

Developed by the IAB Tech Lab as a part of the Project Research effort, the Global Privacy Platform (GPP) has been designed to consistently manage the sharing of any consumer consent signals in a standardised manner so that businesses can more efficiently comply with the various global privacy regulations as they proliferate and evolve across different countries, regions and states.

In practice GPP acts as a singular transmission protocol for real-time transparency and control signals from platforms, sites, apps and users. It has been designed to be open and extensible whilst streamlining technical privacy standards into a singular schema and set of tools which can adapt to regulatory and commercial market demands across channels. Having one single global technical standard will reduce the cost of maintaining and updating privacy controls for users. In particular, the ability for the GPP consent signal to accommodate different jurisdictions will make it a lot easier for the digital media ecosystem to keep up with technical requirements as they evolve.

Benefit to Consumers

Internet users will see incremental predictability in transparency and control over time as privacy and data protection norms converge. Many more users, in countries previously uncovered by powerful digital advertising transparency and control tools, can see into, and have a say over, the various data uses for digital advertising.

Benefit to Publishers, Advertisers and Ad Tech Vendors

Businesses will see reduced cost of maintaining privacy and data protection controls for users across the regions they work in. GPP adopters will be able adapt to any regional changes and the inevitable convergence in privacy and data protection experiences without technology switching costs.

Multi-Jurisdictional Design

The multi-Jurisdictional Design proposal within GPP is to have sections (where sections equate to country or regional jurisdiction) within the GP string, where each section is dedicated to one jurisdiction with legal bases or permissions specific to that jurisdiction. Consent Management Platforms (CMPs) only generate a GPP string section for the jurisdiction(s) that the digital property requests and transmit that information to downstream vendors, along with an indication of the jurisdiction(s) that the digital property will apply. Participants thus make their own determination over how to proceed with the information provided to them via the digital property's CMP.

The proposal builds on the TCF v2.0 concept of a 'TC String', composed of flexible and discrete 'Segments', expanding these to support multiple existing and new privacy formats. Also, similar to TCF string, GPP string is also able to be transported via OpenRTB -and IAB Tech Lab will standardise storage locations and naming for the content of the GPP data and GPP string so that ad tags embedded in mobile apps can also find the GPP data and string in a consistent way.

To read more about these specs simply click here

Global Accountability Platform

In addition to this, The Global Accountability Platform will launch in the second half of 2022. The GAP will check to ensure companies are consistently honouring the consent signals throughout the entire supply chain, from the inception of the data to the delivery of the impression. The core purpose of the platform will be to audit the supply chain and ensure that the 'integrity of the consent string' remains intact.

Conclusion

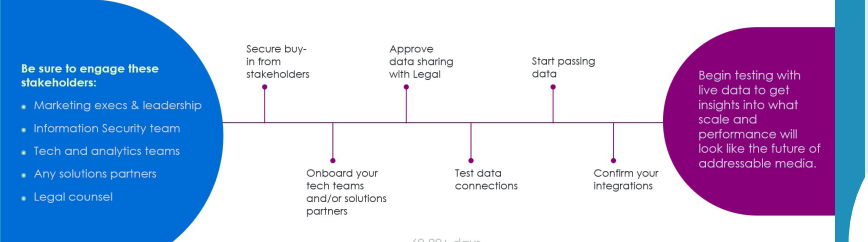
Section 11

This *document* should be used in conjunction with the other recent outputs from the data council *(see 'further reading' links below)* and our recommendations remain very similar.

- Review strategic requirements, both in the short and long term.
- Fully review and assess all the first-party data assets that your organisation has access to.
- Collaboratively engage with any internal stakeholders to align on the organisational approach, related processes and resources required.
- Agree upon the product & technical capabilities required to achieve the strategic aims previously agreed upon.
- Consult on the related privacy requirements, both now and moving forwards.
- Construct a workable framework in relation to the level of access to, and usage permissions for, any consumer first-party data.
- Work with your current technical vendors to fully understand their capabilities, related to your requirements.
- Ensure that you consider both the technical capabilities required as well as scale, as both will be important in practice for the future.
- Review any other options in-market that meet your defined needs to benchmark your current solutions, or options to evolve towards.
- Comprehensively plan for the on-boarding process and consider reviewing the agreed lookback windows for any older data assets.
- Work to execute with excellence with what you have access to in the short term, with both your owned 1PD assets and any second-party assets.
- Allow for Partners to be invited to collaborate without restriction or bias for them to as first be mutual clients of the clean room facilitator.
- Allow for collaboration with any and all data types without restriction. Look to include id graphs, log level data (such as transactions/ad logs/conversions) a wide range of data models, containerised code & mapping files etc.
- Allow for flexibility and interoperability by not limiting the use-cases to only be executed on partner collaborations, or dictating that source data should first be replicated onto vendor infrastructure before collaboration can begin.
- Plan ahead strategically for your plans in the medium-long term and learn to fully leverage your partners effectively.
- Test aggressively in the short term and leverage any findings and insights internally and with key partners.

When should you get started?

You'll need time to get stakeholder buy-in and to onboard your tech teams.



CRITEO

Thereafter it's about relentlessly improving by going back, reviewing all of the suggested approaches in this handbook and further enriching the assets and profiles you are managing on an ongoing basis.

As new data policies continue to globally disrupt of data and marketing industry, all website, app and online store owners must adapt or else get left behind. The scale and quality of your customer-first data is what will set you apart from your competition and provide the optimal value to your commercial partners. All the current global research points to the value of 1PD assets becoming increasingly critical moving forwards (as per the below from eMarketer).

How US Data Leaders Expect the Coming Changes to Third-Party Cookies and Identifiers Will Affect Their Company's Use of Data, 2021 & 2022

% of respondents

	2021	2022
Change our approach to attribution modeling (e.g., model types, teams to run the models)	26%	42%
Expand our engagement with third-party industry groups seeking to build "post-cookie" identity resolution solutions	27%	43%
Increase focus on developing custom/in-house identity resolution solutions	39%	42%
Increase spending/emphasis on contextual advertising	24%	42%
Centralize all customer/customer relationship management (CRM) data into one repository (or begun efforts to do so)	35%	41%
Increase spending/emphasis on use of first-party data	42%	41%
Increase interest in third-party identity resolution solutions	30%	37%
Change our approach to campaign and audience measurement	45%	34%
Conduct an audit of our third-party data providers and other supply chain partners	18%	32%
Increase use of AI solutions for consumer insight development and marketing decision-making	31%	31%

Note: 2021 n=121; 2022 n=125
Source: Interactive Advertising Bureau (IAB), "State of Data Report," Feb 8, 2022

273124 eMarketer | InsiderIntelligence.com

We recommend that media businesses work to keep creating premium experiences and content that consumers love and keep working towards establishing a positive network effect of growth and marketing excellence.

Also, keep accessing any of the regular outputs from the IAB Australia Data Council and related blogs and articles on the IAB Australia website.

Good luck!

Further Reading

In 2021 the IAB's Cross-Jurisdiction Privacy Project released a summary of how the privacy laws of Australia, Brazil, Canada, China, India, Israel, Japan, Mexico, Nigeria, Singapore, and South Korea apply to the digital advertising industry.

https://www.iab.com/wp-content/uploads/2021/07/IAB_CJPP_Compendium_2021-07.pdf

ID Explainer Guide & Matrix of Providers (December 2021)

https://iabaustralia.com.au/resource/identifiers-explainer-guide-and-matrix/

Contextual Targeting Handbook (June 2021)

https://iabaustralia.com.au/resource/contextual-targeting-handbook-2021/

Data Handbook (July 2020)

https://iabaustralia.com.au/resource/data-handbook-2020/