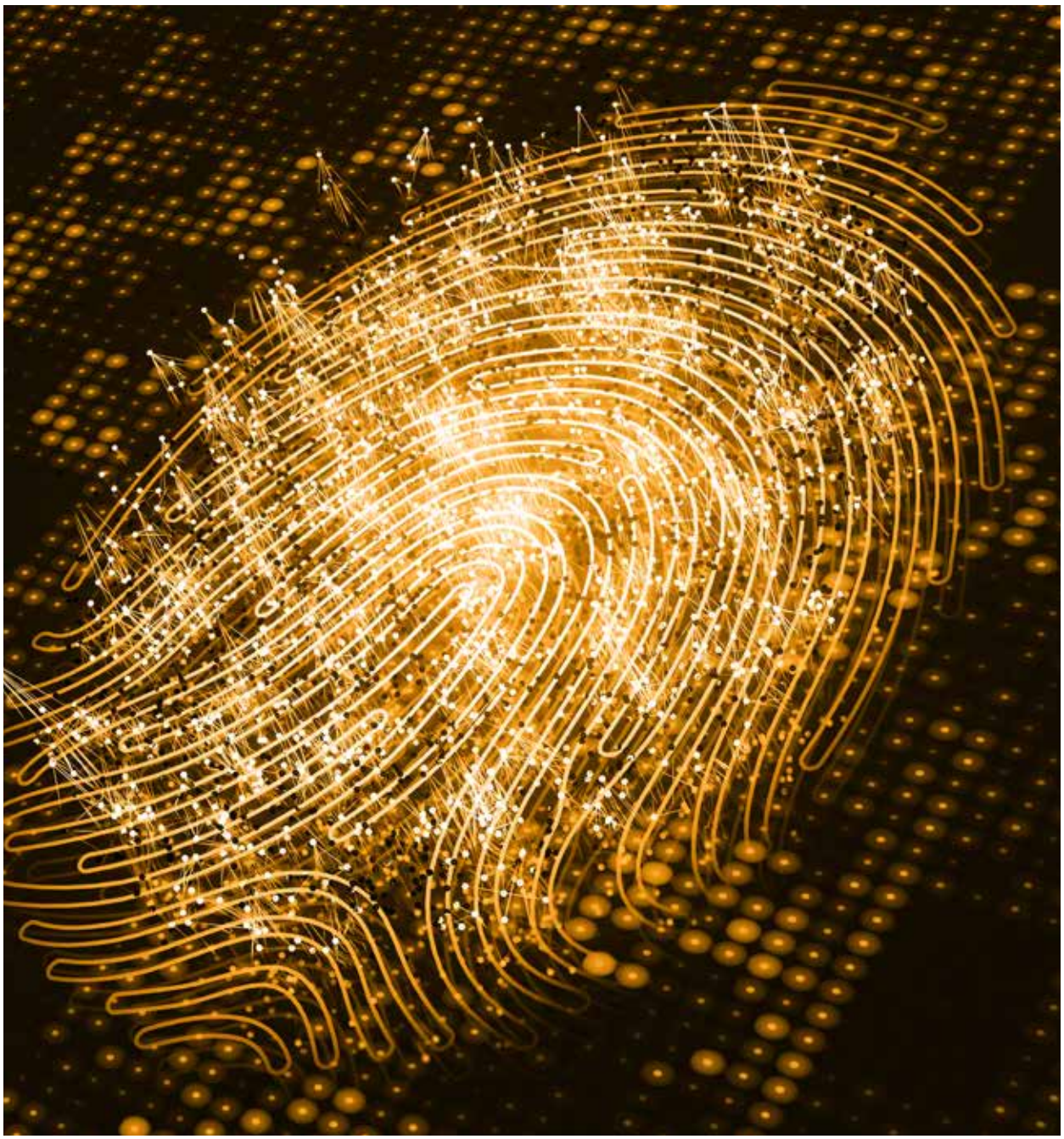
Winterberry Group

JUNE 2020

IDENTITY OUTLOOK 2020

The Evolution of Identity in a Privacy-First, Post-Cookie World



acxiom LiveRamp MERKLE TransUnion

Acknowledgements – This report would not have been possible without the significant contributions of the industry leaders who supported our research and shared their opinions with us. In particular, Winterberry Group is grateful to our project sponsors for their time, efforts and insights:

Premier Sponsors

Supporting Sponsors

In the course of developing this perspective paper on the current state of identity, Winterberry Group spoke to over 100 senior industry experts from both the U.S. and Europe. These experts represented over 60 companies involved in the identity ecosystem, ranging from solution providers, technology and data companies to publishers and law firms focused on privacy considerations.

The objective of this paper is to facilitate understanding of this rapidly evolving market segment, one which we believe can and will continue to be increasingly helpful in marketers' ever-elusive quest to obtain a complete understanding of—and forge connections with—their customers.

WINTERBERRY GROUP AUTHORS

Bruce Biegel
Senior Managing Partner

Charles Ping
Managing Director EMEA

Michael Harrison
Managing Partner

TABLE OF CONTENTS

Executive Summary

As the adoption and application of identity solutions have matured and accelerated, that growth is now challenged by enforcement of the GDPR, CCPA and, most importantly, the final deprecation of third-party cookies. We believe that regulation and cookie deprecation are a positive for the future health and next stage of growth for the advertising and marketing industry as they are appropriate catalysts for change in an increasingly privacy-aware consumer environment.

These factors are forcing innovation among data and technology companies as they seek to replace the current cookie-centric models with new privacy-compliant approaches. Our research has found a set of fundamental adjustments in how the market is expected to evolve over the next three years. However, one of those is not the definition of the terms identity and identity solutions, despite the fact that we heard over 60 different definitions in the course of our research.

In addition to cookie deprecation and regulatory changes, our conversations identified six additional factors that are impacting the identity landscape, including:

- The focus on first-party data is accelerating among both marketers and media owners;
- The explosion in the number of addressable devices at the individual and household level;
- The significant adoption of video consumption and delivery services by consumers;
- The recognition of the value of identity and identity solutions as the center of the advertising and technology stack;
- The impending difficulty in measuring, evaluating and providing attribution; and
- The determination of media owners to recover value.

The growth and adoption of the next wave of identity solutions is expected to vary, depending on the ecosystem that is leveraging it. As a result, it is important to understand the nuance in the way that identity is evolving and is applied.

An Evolving Set of Identity Approaches. For each market segment, the number of unique identity resolution approaches has expanded under today's more restricted and technologically complex set of constraints. Winterberry Group sees these solutions falling into the following five categories:

- A proprietary ID based on first-party data where the brand or media owner has established a unique ID for use on their owned properties and for matching with partners either directly or through privacy-safe environments; leverages a deterministic approach.
- A common ID based on a first-party data match to a third-party, PII-based reference data set in order to enable scale across media providers while maintaining high levels of accuracy; leverages a deterministic approach, with probabilistic matching to increase reach.
- A common identity token used to facilitate enhanced recognition across the programmatic trading ecosystem; leverages deterministic and probabilistic approaches.

We broadly segment the market into three overlapping ecosystems that leverage a blend of identity approaches:

Personalization on Owned Properties
the use of martech solutions centered around CRM databases and CDP solutions to provide personalized experiences across websites, apps and in-store;

Programmatic Digital Advertising
advertising activated through the use of adtech solutions, including DSPs, DMPs, SSPs and exchanges, where 80%+ of digital advertising expenditures are transacted; and

Advanced TV (including addressable TV, CTV and OTT)
where the combination of individual shared identities meet in an extremely fragmented set of solutions that include the programmatic use of identity and approaches to attribution.

- A second-party data environment based on clean environments with anonymous ID linking to allow privacy-safe data partnerships to be created; leverages a deterministic approach.

- A household ID based on IP address and geographic match; leverages deterministic and probabilistic approaches.

Contextual targeting, although not strictly "identity," has re-emerged as a complementary and standalone option in cases where there is limited or no first-party data.

Maturity of Use Cases. The broad use of cookies and the common technology adoption of DSPs, DMPs and SSPs have helped to standardize the advertising market. They have also propelled the use of CDPs and first-party data graphs, which are driving the development of insights by combining the ability to more consistently activate across owned channels and the ability to measure and optimize.

While the most mature use cases today are found in targeting and measurement in programmatic digital media, we also expect to see the greatest disruption here. Additionally, the shift from linear TV advertising into addressable TV, CTV and OTT is serving as a catalyst to drive adoption of emerging identity approaches.

Given the impact of privacy and a faster rate of change expected in the availability of identifiers, we should expect the evolution of use cases and solutions to develop at different rates in different geographies.

- ***Personalization:*** Due to its higher maturity and lower regulatory intensity in the U.S., adoption of identity for personalization efforts will accelerate in U.S. markets through both U.S. and EU vendors.

- ***Programmatic:*** Europe, due to the early adoption of GDPR, is serving as a testing ground for innovation. Many of the identity approaches we are seeing are led from here, even if the companies are headquartered in the U.S.

- ***Advanced TV*** (***ATV***) ATV, the least mature ecosystem and least impacted by the loss of individual identifiers, is the most fragmented identity ecosystem. Given the size and complexity of the U.S. ATV market, this should evolve in the U.S. market more rapidly than in the EU.

Privacy and the Regulatory Outlook. In our interviews with privacy specialists, we heard a consensus that policy will need to be established prior to the industry's ability to clearly define and adopt compliant technical standards. There is strong support to move forward with standards through Project Rearc and the W3C, to the extent possible while policies remain in development over several years.

Our conversations have highlighted two key considerations that companies building and/or leveraging identity solutions should monitor over the next 18 months:

- It is expected that more identifiers will be gradually considered PII within the U.S. system, as initiated by the CCPA, potentially including MAIDs in the future.

- IP addresses, already personal data in the EU, are less likely to be considered PII in the short term, largely due to the attribute's role in non-marketing use cases such as fraud detection.

Brands will leverage first-party identity solutions for personalization while utilizing third-party identifiers to increase recognition and to resolve with the broader programmatic ecosystem. We expect expanded development and use of first-party identity graphs initially by enterprise marketers, with rapid adoption across the mid-market over the next 24-36 months. Within these first-party identity graphs, privacy-compliant third-party data will continue to be used to enhance and/or enrich first-party profiles.

The breadth and availability of first-party data assembled from offline sources and online devices will create the opportunity for advanced machine learning/AI-based decisioning, channel orchestration and customer journey management. In turn, this will create demand for more integrated platforms to support the personalization on owned ecosystems.

Publishers. The consensus view clearly indicates that the center of the new programmatic ecosystem will also be based on first-party cookies and other first-party data. However, this ecosystem will leverage the broadest set of identity solutions in order to achieve both scale and reach while maintaining the desired level of accuracy. The five different identity solutions identified earlier (plus contextual targeting) can be applied to

Marketers Will Apply a Blend of Approaches Going Forward.

The conclusion that Winterberry Group draws is that multiple identity solutions will be required and will continue to evolve in parallel.

different media offerings based largely on the availability of first-party data, audience volume, frequency and depth of engagement.

With publishers having lost much of their ability to optimize the monetization of their content and audiences, this evolution provides the best opportunity for them to recapture revenue from both subscriptions and advertising. It was also clear from our conversations that there is no support voiced for a single ID solution to rule above all others.

The Advanced TV ecosystem utilizes a combination of individual and household data. The fluid nature of viewing behavior across shared and individual devices provides an expanded set of identity opportunities for targeting and measurement/attribution. The identity opportunity is expected to remain complicated due to the fragmentation of data origination and control amongst infrastructure, device and content controllers.

We expect competition for advertising dollars to be split between two programmatic identity approaches: one targeted at the individual and their personal device (and their first-party data) and the second targeted at either the individual or the household on shared devices. We expect that identity solution providers who are building both deterministic and probabilistic approaches to Advanced TV identity graphs will provide a bridge between these data environments.

Whilst some technology approaches may span multiple geographic territories, the segmentation of the media industry by language and country indicates that it is **highly probable that identity solutions will see country-level adoption**, with a combination of single publisher ID support and a collaborative model to create scale.

Additional Takeaways for Consideration

- ***First-party data and identity graphs will need to scale:*** In addition to volume, accuracy should be placed at a premium in constructing the first-party graph. The use of partnerships between brands—and between brands and media owners—will enable enhanced scale to be leveraged across use cases.

- ***Co-operation is critical to beat the scale of walled gardens:*** Co-operation is a key part of the future, whether through publishers grouping together to generate scale or through media owners and advertisers participating in ID sharing technologies.

- ***Measurement and attribution will become more challenging:*** Measurement and attribution are going "back to the future" to build insights on a broader canvas of data feeds and identity solutions. MTA solutions will remain at the top of marketers' desired data and identity capability wish lists. However, fragmentation across the different types of gardens will remain a challenge.

- ***Organizational talent gaps:*** The lack of coherent approaches within marketer/agency organizations across advertising, marketing and commerce groups may hinder the adoption of holistic privacy-compliant identity options.

- ***Complexity may lead to a deeper review of in-housing***: In-housing has grown in an environment when it was possible to implement a limited number of established tools to manage media within a stable and growing economy. In the emerging identity market, the implementation of identity solutions and a more complex media planning and buying ecosystem is likely to result in a pause in the shift to in-house models.

In conclusion the factors driving focus on a new set of identity solutions, the significant value of advertising spend, business objectives that are supported by a focus on consumer engagement and the determination by the industry to find a better, more privacy-compliant path forward will all come together to drive adoption.

We believe three things to be true in what comes next:

No one solution will rule them all.

There will be significant investments in evolving to a first-party world across data, people and technology.

While AL & ML decisioning solutions will provide the brains for the next generation of advertising and marketing solutions, identity will remain its heart.

RE-EXAMINING IDENTITY

The adoption and application of identity in marketing and advertising have rapidly expanded in the U.S. over the last two years. The amount of data being generated, the privacy constraints applied and the capability for managing, analyzing and decisioning with that data has grown exponentially. This expansion has also included the number and type of use cases, the breadth of technology and the services options across adtech and martech.

SIX CRITICAL FACTORS

> "Identity is the core part of so many use cases. More than anything, where identity has evolved to today from where it was [a few years ago] is a deeper embrace of and larger emphasis on devices, mobile apps and CTV. You see a much bigger embrace of identity to drive and power advertising."
>
> *– SVP, Demand-Side Platform*

Given the implementation of GDPR, the pace of identity's adoption and the trajectory of its evolution has differed across European territories. Against this background and in the midst of continuing regulatory interventions and evolving browser policies, the identity landscape is likely to see significant change by the end of 2021. From our conversations, we believe there are six (6) critical factors that are impacting the identity landscape, including:

- The explosion in the number of addressable devices at the individual and household level. In 2018, the average number of addressable devices per person was 3.5; today, that number is predicted to be between 6 and 8. At the household-level, the average number of connected devices is at least 13, but only 8 are addressable/marketable and therefore matter to the advertisers and publishers.
- The continued deprecation of third-party cookies, starting initially with Safari and Firefox and finally announced by Chrome in January 2020 for elimination by no later than the end of 2021.
- The significant adoption of video consumption and delivery services by consumers, leading to a corresponding shift of media advertising expenditures and the related advancement of programmatic buying solutions in addressable TV, OTT and CTV (collectively referred to as Advanced TV).
- The recognition of the value of identity solutions in driving performance and consumer engagement across channels and touchpoints. This recognition is demonstrated by the market's increased adoption of adtech and martech solutions with identity at their core.
- The impending difficulty in measuring, evaluating and providing attribution across marketing and advertising campaigns due to the loss of third-party cookies, which will severely impact the ability to optimize efforts.
- The efforts by media owners to recover value and rebalance control against a programmatic trading system that they feel has undervalued their investment in content origination.

The adoption and changes in the use and application of identity, along with the expanding number of market participants, has led to a rethinking of the current state and outlook for identity and identity solutions.

What is "Identity?" The Term Remains Amorphous as the Industry Has Yet to Align on a Single Definition

"I think broadly the concept boils down to the idea of addressability and bringing together data assets to understand a consumer from a targeting or analytics standpoint. Identity is the central dataset that allows you to aggregate disparate data points to understand who you want to contact and how."

– CEO, Data Provider

"For me, identity is static information on an individual that can always lead back to that person. Identity allows you to be connectable and relatable, but not necessarily "known." .... When we talk about identity, what we really want to do is [enable marketers to] display consistent and meaningful messages directly to consumers."

– Chief Privacy Officer, Data Services Provider

"Identity to me would be, a consistent way to track an individual with longevity across various channels, with the goal of targeting and measuring the impact of marketing campaign influence."

– Chief Data Officer, Agency

"Identity is any kind of token that can be applied back to a person or household"

– VP of Product, Connected TV Provider

"Identity is the ability to connect disparate identifiers to a comprehensive view of a customer. For B2C, it is a consumer. For B2B, that could be an account or a persona of an account."

–VP of Product, Identity Resolution Provider

"Identity allows us to differentiate between drive-by consumers of free content on our sites and authenticated users in the subscription world."

– General Manager, EU Publisher

"Identity in the context of advertising is about giving users a better, more relevant experience. There is no single definition for identity, whether it is cookies, sign in, single identifier, etc. But, at its core, identity-based advertising is being able to resolve down to users or see users as one."

– Global Privacy Lead, Programmatic Solutions Provider

"If you take the customer-centric view, identity is a pathway to intelligence and is not just the identifiers but the descriptors as well. It is all of the things linked to an identifier that can describe a person."

– Product Officer, Customer Data Platform

What is Identity?

Is there a new definition of identity?

Winterberry Group does not believe that there is a new definition since we published our last paper on the topic in 2018. However, we have observed confusion in the market due to an increase in the number of market participants (including data, technology and privacy professionals), as well as an increase in the number of approaches to identity solutions.

The most common point of confusion is the difference between data and identity—terms which are increasingly used interchangeably. In the world of marketing and advertising, an identity represents a combination of data elements (sometimes referred to as attributes) that describe a person or a household.

Does the meaning of identity vary according to perspective and geography?

Yes. There are two main views of what identity means: as an email/name/address-connected concept or as an individual behavioral trail. This distinction is driven by the different definitions of personal data/PII by European and U.S. regulatory bodies as well as by the availability of a linkage to offline data. While the two geographies may converge with the "GDPR-ization" of global marketing data, differences are likely to remain. The winds are blowing but the rate of change is unknown.

The misalignment in definitions carries over into how territories think about the relationship of PII/Non-PII to households and people. In the U.S., PII is about people, not households, and this means that household-level data is generally not considered PII. Whilst a household is not considered personal data in Europe, it can be treated as personal data in the territory if/when household information is combined with personal data.

WINTERBERRY GROUP DEFINES IDENTITY AS:

The effort to recognize and understand individual audience members (including customers, prospects and other visitors) across channels and devices such that brands can interact with those individuals in ways that are relevant, meaningful and supportive of overarching business objectives.

WINTERBERRY GROUP DEFINES IDENTITY SOLUTIONS AS:

The coordinated activation of platforms, data and supporting services (both provided by third parties and sourced from among marketers' in-house resources) that support persistent recognition of audience members across all devices and other promotional and transactional touchpoints.

The greatest difference in definition is between "PII," "Non-PII" and "Personal Data:"

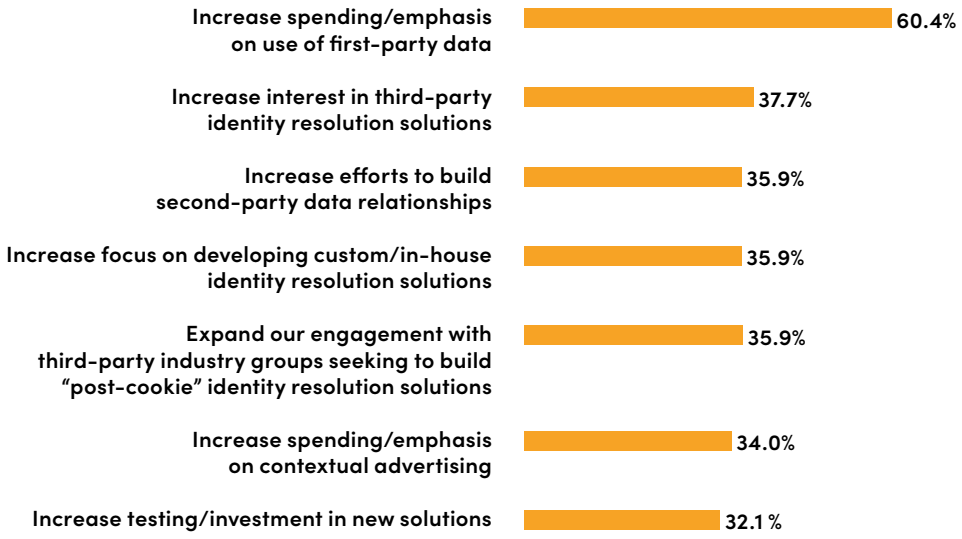
"PII" (Personally Identifiable Information):
the term traditionally used in U.S. markets to describe data elements that directly identify a person, such as name, address, phone number, email address, SSN and a limited range of other identifiers.

"Non-PII":
any element that does not directly identify an individual. In the U.S., this includes proxy identifiers such as cookies, MAIDs, IP addresses and other identifiers that may be unique but do not allow direct recognition of the individual.

"Personal Data":
the term used under GDPR that has a much wider scope than "PII" because it includes data elements that may identify individuals when combined with personal data. This means that IP addresses, MAIDs, specific latitude/longitude elements, cookies and device IDs are generally accepted as within the legal remit of GDPR.

How Do First- and Third-Party Data —and Cookies—Play Into Identity?

"Google and other major browser developers have recently announced plans to discontinue support for third-party audience cookies through their respective platforms. How do you expect this change will affect your use of data?"



Note: Multiple responses allowed; not all answer options are shown

Source: IAB/Winterberry Group State of Data 2020

First-Party Data and First-Party Cookies

The aggregation of first-party data is critical to building direct relationships with consumers and driving value with enhanced customer engagement. It is only natural then that the digital equivalent is the first-party cookie. These cookies are set specifically by the domain that a visitor is on and cannot be set by anyone else. The consumer has a reasonable understanding that this will happen (whether or not they read any privacy notice), and the rights granted through consent provide the brand or media owner with the ability to leverage the data contained or linked for marketing and advertising use cases.

Third-Party Data and Third-Party Cookies

While there is no such thing as a second-party cookie (so far), the industry has made extensive use of third-party cookies. These cookies are set by companies that do not own or control the domain that the visitor has reached. It is extremely difficult for a casual visitor to understand what third-party cookies were set on their local device without a detailed reading of a privacy notice.

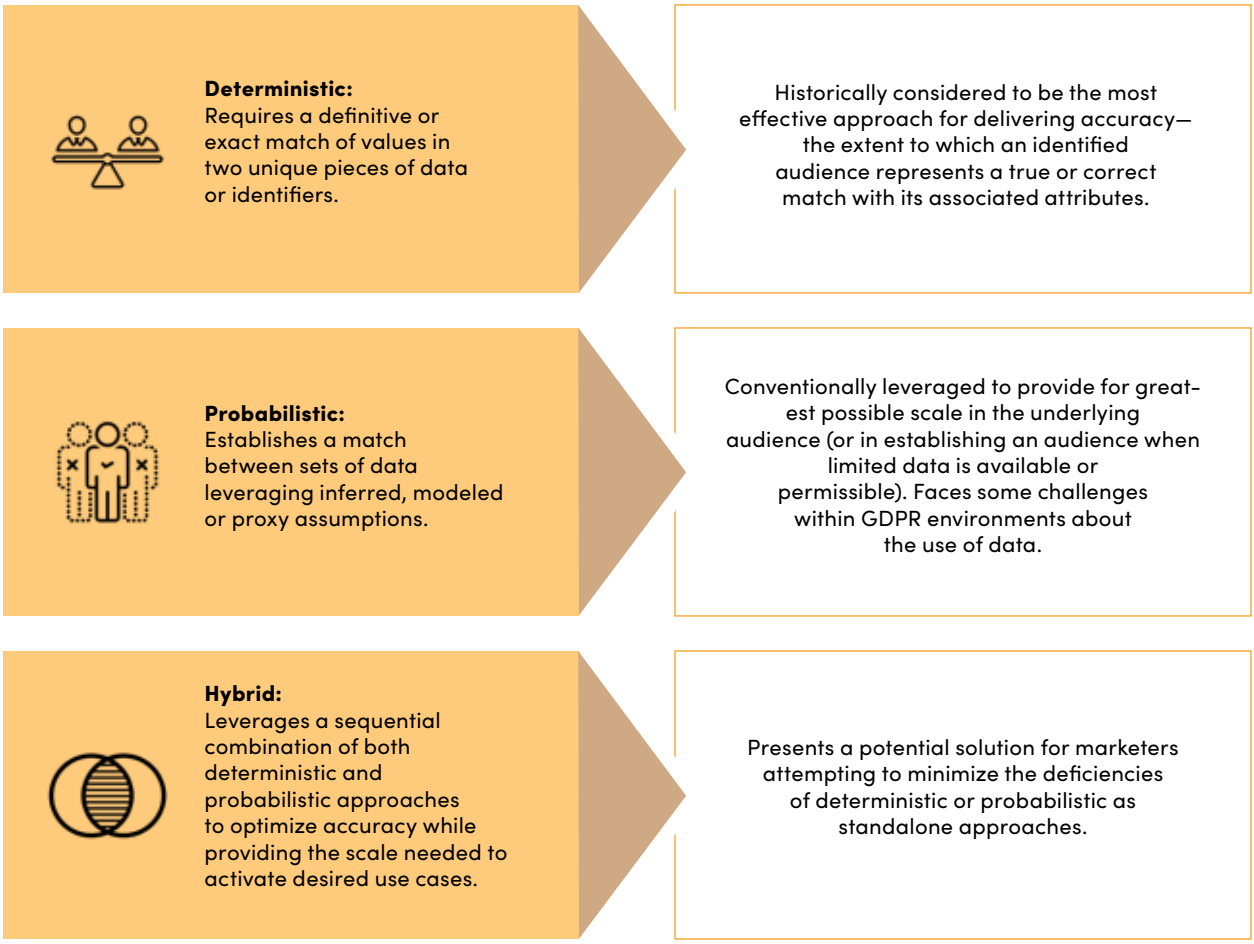
Third-party cookies are used to understand consumer behavior across multiple websites, building a more comprehensive picture of consumer interests. These have been removed by Firefox and Safari, and are expected to be deprecated by Chrome by the end of 2021. This will severely limit marketers' and advertisers' ability to widely track, target and attribute individuals across the web.

Third-party cookies are not the same thing as third-party data. Third-party data may be collected (compiled) by an entity with a direct relationship with the consumer, derived through public sources, assembled via models or licensed from other third parties. Crucially, however, third-party data is used by companies without a direct consumer relationship. Licensed in the digital ecosystem through a data store, third-party data is used in targeting, enhancement, enrichment, measurement and other use cases.

How is Identity Different from "Onboarding?"

Onboarding, one of the first identity solutions to come to market, is the process of linking first- or third-party data to a cookie. Competing solutions in market are differentiated principally by their reliance on Deterministic, Probabilistic or Hybrid methodologies for completing this process.

Matching Approaches Used in Identity



The reason that different approaches are used is that the ability to match deterministically is typically restrained by the need for smaller, more accurate data sets where PII serves as the primary match key. As marketers seek to extend the data set, they use modelling techniques to infer connections. This probabilistic approach will allow the marketer to gain scale, but will reduce accuracy. Of note: accuracy itself may vary even within deterministic, as a match can be true but not precise (such as in the case of shared logins).

The implementation of GDPR has made third-party data in Europe harder to collect and to onboard. Winterberry Group has observed that third-party data assets, while still highly valued, are more limited in Europe given the removal of non-compliant assets from the market. Additionally, limitations on the period of time during which data may be retained have led to a significant reduction in scale—but with a corresponding increase in accuracy. With fewer restrictions under CCPA and other state regulations, the third-party data market in North America has been far less impacted and is expected to sustain its relevancy in the digital ecosystem for the foreseeable future.

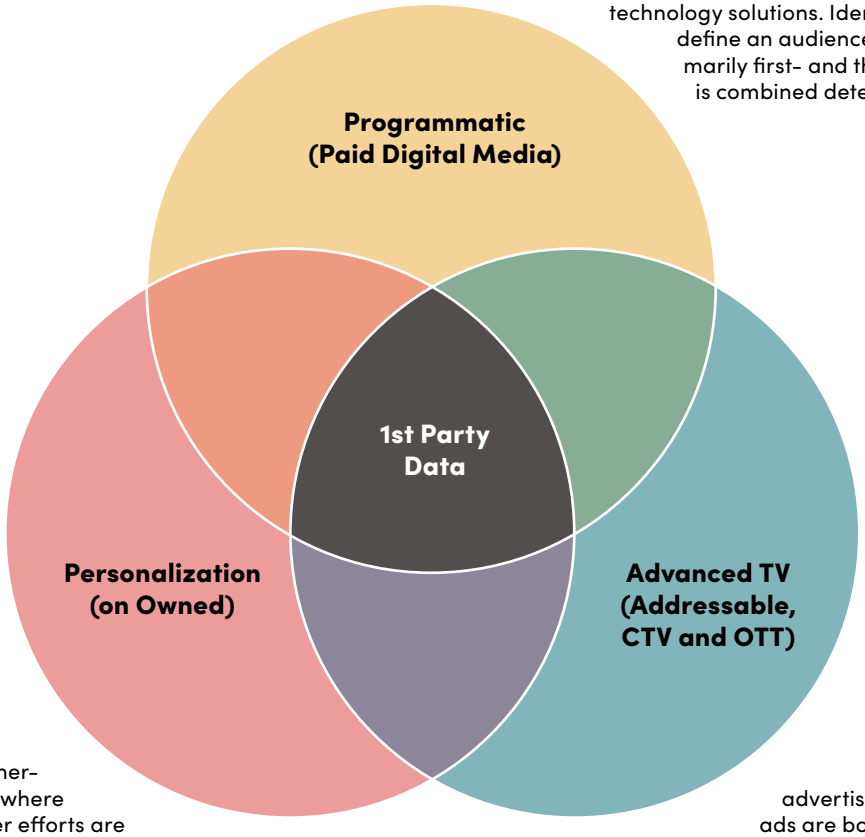
How Do Different Segments of the Market Use Identity?

Each marketing and advertising channel has different regulatory rights—and objectives—when it comes to the use of identity data. As a result, there is significant variance in the way that identity is applied. However, it became clear via our conversations with market participants that many of the different opinions about identity converge based on the channel and use case of that marketer/supplier.

From this, Winterberry Group has segmented the market into three high-level ecosystem groupings. While there is overlap, the demands of Personalization on Owned Properties, Programmatic Digital Advertising and Advanced TV (including addressable TV, CTV and OTT) each perceive identity from its own set of constraints, based on the challenges specific to each sector.

Primary Ecosystems Where Identity Is Used In Marketing And Advertising

Audience-based advertising use cases where ads are bought and measured across media websites, apps and digital-out-of-home via programmatic technology solutions. Identity profiles used to define an audience are built using primarily first- and third-party data that is combined deterministically and/or probabilistically.



Individual consumer-based use cases, where brand or publisher efforts are focused on personalizing the experience on owned properties, including websites, apps and in physical locations. Profiles always start with first-party data that may be enhanced or enriched by second- or third-party data.

Audience-based advertising use cases where ads are bought and measured across addressable TV, CTV and OTT. Identity profiles may be individual or built at the household level and leverage first-party and third-party data sets.

THE EVOLUTION OF IDENTITY SOLUTIONS

In today's market, cookie-based matching (whether first- or third-party) is the dominant approach to individual-based identity solutions. Postal and/or IP address-based matching has been the primary approach for household-based identity solutions.

As a result of previous and pending regulatory and browser changes, three significant developments have occurred in identity solutions over the past two years:

The recognition that **privacy-by-design and consent** are crucial elements for identity and must take place before data is sourced and ingested in order to create a base that is compliant with regulations.

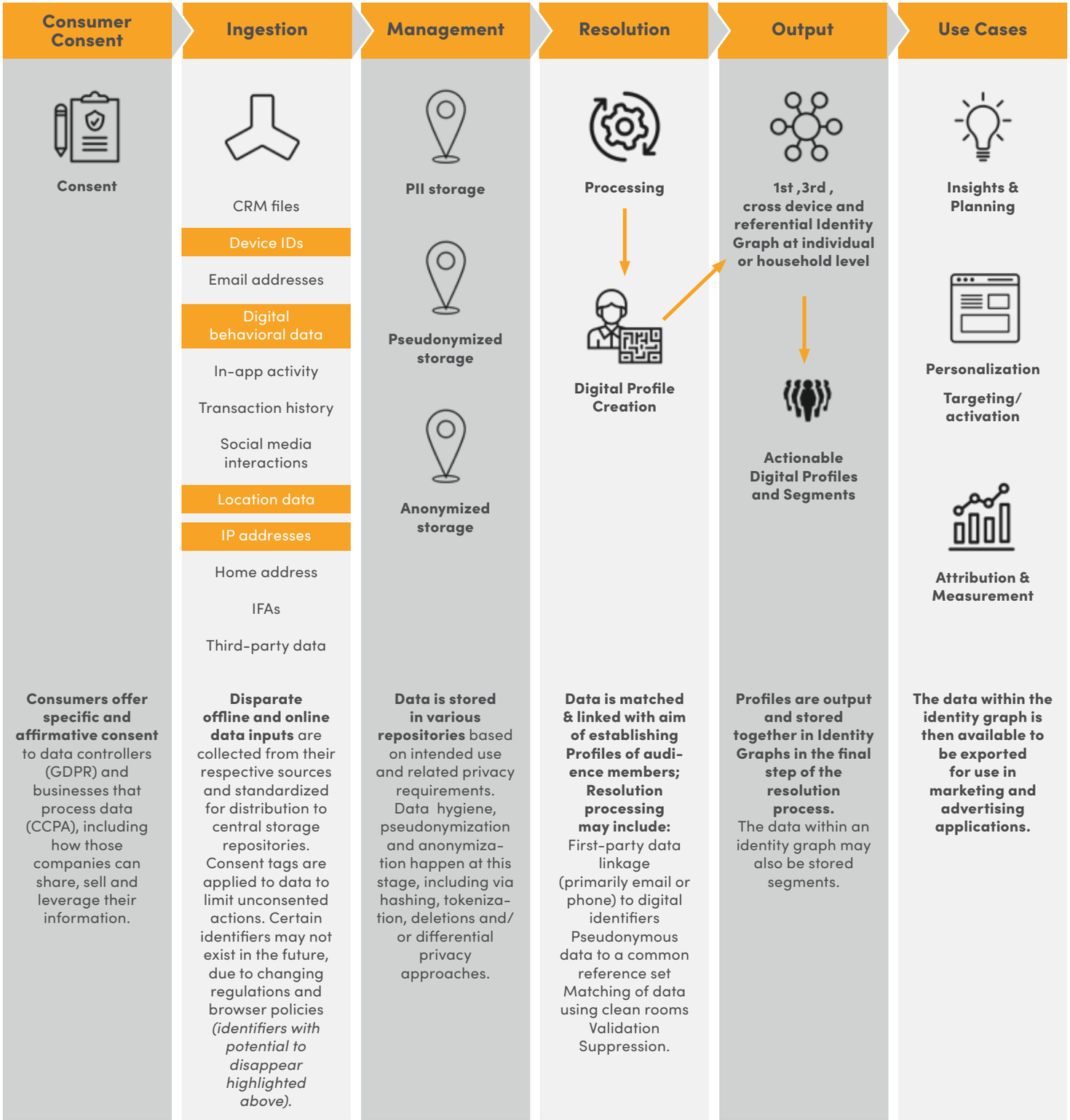
The **development of five unique identity resolution approaches**, each at various stages of market evaluation and adoption, which are not dependent on third-party cookies.

The **expansion of the definition and composition of identity graphs** (the output database of profiles, devices and other identifiers), as well as their use across differing ecosystems.

The diagram below shows how the identity solution process has evolved over the last two years to its current state with consent at the beginning of the process to create compliance and changes in both identity resolution and identity graph creation.

> We see some [identity] providers doing consent management, because consent is now a critical part of identity.
>
> *– Senior Director, Managed Services Provider*

The Identity Solution Process Flow



Privacy-by-Design and Consent

Since our last paper, we have seen identity solutions being built with privacy at their core. Providers—and marketers—are recognizing that there needs to be a balanced and fair consent capture process at the start of any identity effort. This was a move away from the asymmetric approach that previously existed, which leveraged a streamlined opt in procedure and a highly complicated opt out process.

In addition to this balancing of consent procedures, the technical approaches to restricting identification have not only grown in complexity, but also gained in clarity—with greater market understanding of the nuances. Technical approaches include:

Differential privacy:
An approach to eliminating re-identification of data through the addition of extra "noise" formed of incremental, unrelated data.

Pseudonymization:
a technical approach to the de-identification of data done by replacing elements or the whole field with pseudonyms. Various software applications allow for the pseudonymization of data and separate out the newly de-identified data from the key that was used. The data can be re-identified only with that key. Pseudonymized data is considered personal data within GDPR unless the user has no current or future access to the key to allow re-identification.

Anonymization:
a technical approach that can never re-identify a person. This may be because the key used has been destroyed or that the method to anonymize is random. The risks of re-identification from anonymous data need to be carefully considered when multiple attributes are still linked to the data – especially when audience sizes are small.

> "The second-most prevalent question we get is: "How can you ensure the data is compliant?" There are more and more questions around third-party data assets. There is a huge opportunity for companies that can provide the right privacy-by-design. Companies that have a history of collecting and using data ethically will be in a good place."
>
> *– Managing Director, Identity Solutions Provider*

Finally, identity providers are leveraging an ever-growing list of methods to resolve the privacy challenges of sharing first-party data, such as clean rooms, bunkers, differential privacy and other forms of safe environments that are designed to provide data security.

The Evolution of Identity Resolution Approaches

As privacy has become more important in the ecosystem, and in preparation for pending regulations, the number of unique identity resolution approaches has expanded. Operating under a more restricted and technologically complex set of constraints than the original identity solutions, these solutions have evolved based on the data that is available and that has permissible uses. They also serve the crucial purpose of generating greater flexibility within the first-party domain of brands and publishers. Winterberry Group sees these solutions falling into the following five categories:

A proprietary ID based on authenticated first-party data where the brand or media owner has established a unique ID for use on their owned properties and for matching with partners either directly or through privacy safe environments (e.g.: Facebook, Google, Amazon).

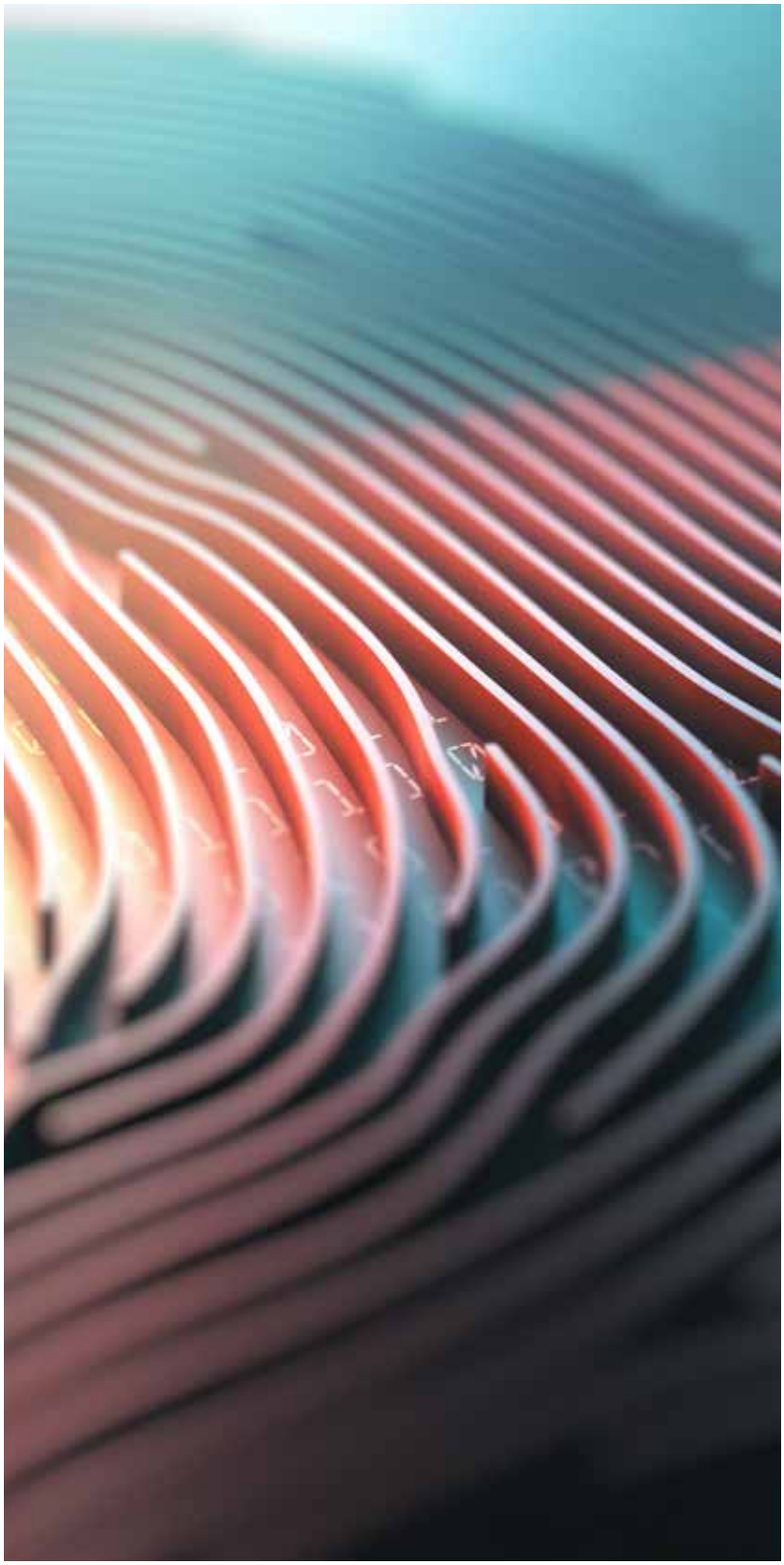
A common ID based on a first-party data match to a PII-based reference data set in order to enable scale across media providers while maintaining high levels of accuracy.

A common ID based on a first-party data match to a third-party, PII-based reference data set in order to enable scale across media providers while maintaining high levels of accuracy; leverages a deterministic approach, with probabilistic matching to increase reach.

A second-party data environment based on clean environments with anonymous ID linking to allow privacy safe data partnerships to be created.

A household ID based on IP address and geographic match*.

*Note: See "Regulatory Implications & Browser Responses" paper section for more information on the regulatory risks associated with each approach



The Expansion of Identity Graphs

The assembly and management of profiles has undergone expansion based on the type of identifiers that are leveraged. These graphs are designed to reflect the new standards of consent and privacy.

Type	Definition	Advantages, Privacy Management & Rights
First-Party ID Graph	A database of profiles comprised of deterministic, first-party identifiers and attributes (including email addresses, phone numbers, account usernames, etc.)	■ **Enhancement:** Third-party data allows marketers to garner insight and target existing customers through the addition of first-party data ■ **Quality/Compliance:** Data collected is consented and aligns with browser and regulatory changes ■ **Control:** Publishers/marketers will have control and opportunity for customization within the first-party domain
Third-Party ID Graph	A database of profiles built on third-party sourced identifiers and attributes assembled from online and offline sources; data is often linked with first-party data using deterministic or probabilistic techniques	■ **Enhancement:** Third-party graphs allow marketers to garner insight and target customers through the addition of first-, second- or third-party data ■ **Quality/Compliance:** Data needs to permissioned and auditable for third-party usage ■ **Control:** Marketers licensing third-party ID graphs may have more limited rights to and control of the data
Cross-Device ID Graph	A database of devices that have been deterministically or probabilistically linked based on the available identifiers to expand the view of the behaviors of that set of devices, including location. May be linked to an individual or household as part of a third- or first-party graph.	■ **Enhancement:** Cross-device ID graphs allow marketers to garner insight, target customers and provide attribution across channels through the linkage of devices to first- or third-party profiles ■ **Quality/Compliance:** Consent is provided for device information through websites, in-app or manufacturer/OS provider ■ **Control:** Licensees are assigned specific rights from the company that assembles the cross-device graph

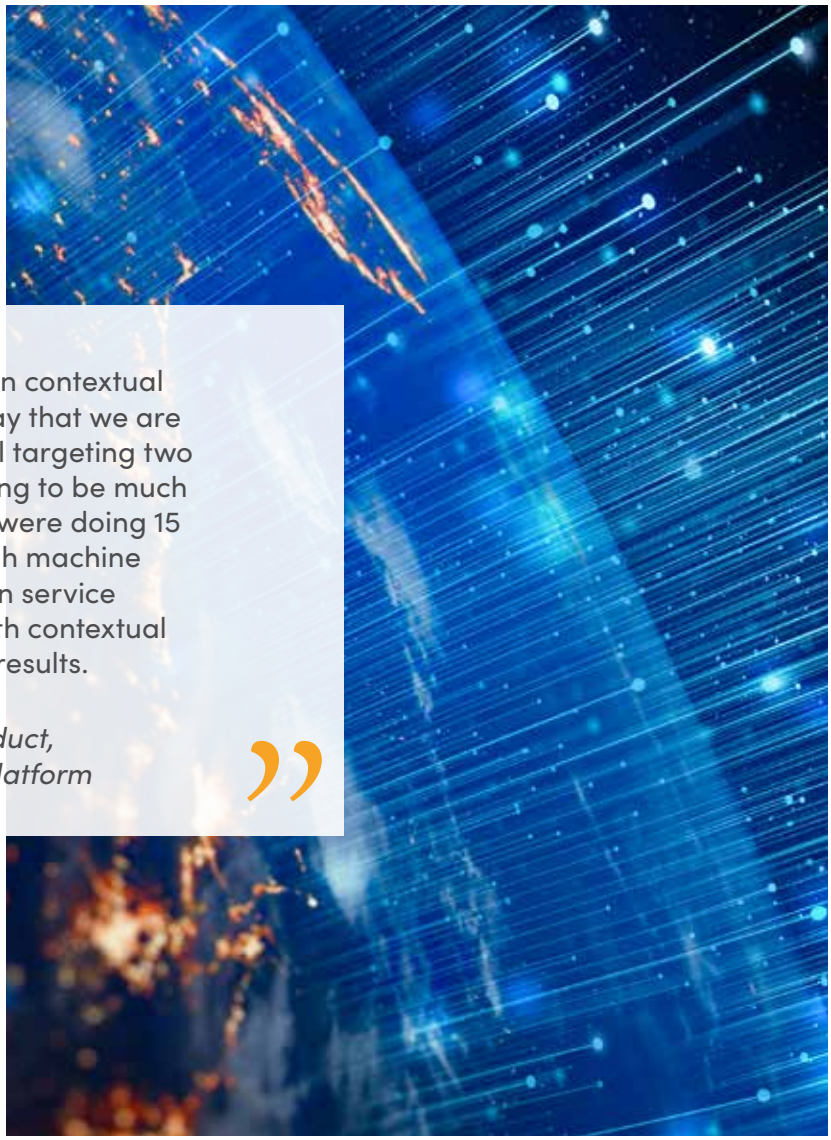
The Rise of Context as a Complement and Substitute to Identity-Based Targeting

Contextual targeting is not new but, in recent years, has become a secondary approach for targeting as third-party cookie solutions ascended.

There are two approaches commonly used in contextual targeting. Keyword contextual targeting matches keywords on a page to determine suitability for ad placement. Semantic contextual targeting refers to showing ads that capture the "meaning" of a page.

As third-party cookies have continued to be restricted, contextual targeting solutions are increasingly substituted for audience-based solutions. This in turn has accelerated the application of contextual approaches, including the emergence of solutions that leverage machine learning to build faster analytical links between content and potential outcomes (sometimes referred to as augmented contextual targeting). In some cases, contextual providers are combining these techniques with privacy-enhancing edge processing to deliver even greater compliance.

In our conversations across the industry, there was consensus that contextual targeting—although not an identity approach—would see further expansion over time both as a complementary solution for identity and as the primary solution for many of the media owners who occupy the long tail (where there is a gap caused by the lack of identity).



> "We're seeing a rise in contextual targeting, and the way that we are going to do contextual targeting two years from now is going to be much better than what we were doing 15 years ago. Through machine learning, you can service real-time signals with contextual signals to get results."
>
> *– VP of Product, Supply-Side Platform*

THE MATURITY OF AND OUTLOOK FOR IDENTITY USE CASES

Our conversations have identified three primary use case areas associated with the utilization of identity and identity solutions: insights/planning, activation/targeting and measurement/attribution.

Given the doubling of spend on identity solutions in the U.S. over the last two years—to a pre-COVID-19 estimate of $1.2B in 2020—it is not surprising that many of the use cases that were maturing at the time of our 2018 paper have since matured within the cookie-based identity framework. Yet the likelihood of being able to leverage identity to activate these use cases will change over time, depending on potential regulatory and browser changes.

Personalization (on Owned)

Due to their higher maturity and lower regulatory intensity in American and European markets, marketing and personalization use cases are least likely to be impacted by the deprecation of third-party cookies because they are built off first-party cookies and data derived from their own domains and properties.

Purpose	Use Case Type	Definition	Current State	Regulatory Impact	Post-Cookie Impact	Future Outlook
Insights & Planw	Audience Insights and Segmentation	Leverage audience information including CRM, digital behaviors, demographic information and declared and inferred interests, among others, to garner insights into consumers and create segments	●	○	○	In the marketing environment, this is primarily based on PII enhanced with digital behaviors and not based on cookies
Insights & Planning	Audience Suppression	Remove select audience members and segments from marketing campaigns in order to improve the likelihood that only interested/ relevant consumers will receive a specific piece of marketing	●	○	○	This is reliant on first-party cookies and data, not on third-party solutions
Activation	Email Personalization	Leverage audience behaviors and attributes to personalize email content and customize product recommendations to meet audience interests and needs	●	○	○	Email personalization should see an increase in utilization because brands and publishers are using more emails and collecting more first-party data–thus creating a stronger linkage of first-party cookies and emails
Activation	Improved Customer Service	Allow for consistent customer service across all touchpoints (on websites, via email, within the call center, etc.) to develop a better understanding of customer journeys and brand interactions	◑	○	○	There are gaps in the connectivity of identity solutions and customer servicing platforms that we expect to be resolved as first-party identity usage moves across enterprise applications
Activation	Personalization on Owned Websites	Provide audience members with tailored content and offers on company's owned property	◑	◑	◑	It will become increasingly difficult with the loss of third-party cookies to recognize unknown/ unauthenticated visitors and to provide personalized offers and content to those audiences
Activation	Personalization on Owned Apps	Provide app users with tailored content and offers within a company's owned app (based on first-party relationship)	●	○	○	Given its reliance on first-party data and identity graphs, we expect accelerated adoption for this use case across geographies
Measurement & Attribution	Measurement & Attribution	Overlay owned digital campaign exposure data with CRM and purchase data to measure results	●	○	○	This approach relies on first-party cookies and data in order to provide match back analysis

Immature/Low Impact = ○ Maturing/Medium Impact = ◑ Most Mature/High Impact = ●

Programmatic (Paid Digital Media)

These use cases are fairly mature, and publishers/marketers who authenticate users or target using mobile/location data will be least impacted by the latest regulatory and browser changes. But for most of the programmatic marketing ecosystem, the deprecation of cookies will significantly reduce marketers' ability to activate, plan and measure efforts across third-party domains and anonymous devices.

Purpose	Use Case Type	Definition	Current State	Regulatory Impact	Post-Cookie Impact	Future Outlook
Insights & Planning	Audience Insights and Segmentation	Leverage audience information, including known and anonymous data such as digital and purchase behaviors, demographics, psychographics and declared or inferred interests, among others, to provide insights into and create segments	●	◑	●	The dependence on third-party cookie-derived data makes planning and segmentation extremely exposed through the loss of both counts and attributes used in planning
Insights & Planning	Audience Suppression	Remove select audience members and segments from marketing campaigns in order to improve the likelihood that only interested/relevant consumers will receive a specific piece of marketing	●	◑	●	Suppression is cookie-dependent for both accuracy and reach and will require the stitching together of alternative identifiers to compensate for the loss of cookies
Activation	Location-Based Targeting (Near Venue)	Using mobile, location and device data to deliver content to unauthenticated visitors and/or customers with offers and messages when they are in the vicinity of a certain location (near digital signage/digital OOH, public spaces, etc.)	◑	◑	○	There is a bifurcation between U.S. and European regulations in the ability to use precise location. While the impact of post-cookie is limited, any deprecation of MAIDs will have a high impact
Activation	Online-to-Direct Mail Targeting (Unauthenticated)	Retarget audiences that visited and did not authenticate on digital properties via offline marketing methods such as direct mail outreach	◕	●	●	Primarily a U.S.-based product and requires third-party cookies or high-precision location data, such that the loss of either will be highly impactful
Measurement & Attribution	Measurement and Attribution	Overlay paid digital campaign exposure data with CRM and purchase data to measure results	●	◑	●	This use case is reliant on a combination of MAIDs and cookies to provide identifiers for current solutions. With the loss of cookies, identity graphs will lose coverage and depth in attributes, resulting in the redevelopment of attribution models. In the EU, GDPR has already forced industry participants to adjust their approaches with the potential, over the longer term, to have a similar impact in the U.S.
Measurement & Attribution	Location Based Measurement and Attribution	Overlay mobile, location and device data with CRM, purchase data and location-based data to measure results of location-based campaigns	◑	●	◑	Whilst location can be delivered in very precise formats, the ability to utilize this information is dependent on graphs built with the help of third-party cookies and subject to regulations currently in Europe and potentially in the U.S.
Measurement & Attribution	Online-to-Offline Attribution	Overlay owned and/or paid digital campaign exposure data with in-store CRM/purchase data to measure results	◑	●	◑	This is reliant on a combination of location data provided through MAIDs, IP addresses and third-party cookies. With the loss of third-party cookies, the ability to connect online behavior to location will be greatly hampered. In addition, location data is currently subject to regulation in Europe and potentially in the U.S.

Immature/Low Impact = ○ Maturing/Medium Impact = ◑ Most Mature/High Impact = ●

Advanced TV

This area is the most fragmented in terms of identity solutions and uses but represents the largest opportunity for growth within the post-cookie identity world. Linear and addressable TV has historically relied on household-level data from cable systems and MVPDs—not cookies from internet browsers. However, the impact of cookies for "connected TV" is largely dependent on which device the content is being consumed on; for desktop viewing, the impact is going to be much higher than over mobile or "big screen" TV viewing which relies more on MAIDs and IP addresses, respectively.

Purpose	Use Case Type	Definition	Current State	Regulatory Impact	Post-Cookie Impact	Future Outlook
Insights & Planning	Audience Insights and Segmentation	Leverage audience information— including CRM, viewing and digital behaviors, demographic information and declared and inferred interests, household information and content—to group customers at the individual and household level into segments	●	○	◑	Planning data has significantly improved in scale and accuracy over time as opt-in panels expanded and have leveraged MAIDs, IP addresses and Wi-Fi information. In the event that MAIDs and/or IP addresses are deprecated, planning may be significantly impacted
Insights & Planning	Audience Suppression	Remove select audience members and segments from marketing campaigns in order to improve the likelihood that only interested/relevant consumers will receive a specific piece of marketing	●	◑	◑	Suppression in addressable TV is conducted via "clean" environments syncing first-party data. While connected TV leverages MAIDs and IP addresses, the onboarding process still relies on cookies as a foundation for the identity graph. In a post-cookie environment, suppression precision will be impacted for connected TV
Activation	Addressable TV Ad Targeting	Programmatically serve ad content to different audience segments watching the same linear (VOD) TV program, based on behavior, interests and attributes	◑	◑	○	Addressable TV ad targeting is not based on cookies; it is primarily based on household identities that are provided by the TV and set-top box manufacturers, cable systems, streaming media players and specific channels (which result in a very fragmented targeting environment)
Activation	OTT and "Connected TV" Advertising	Programmatically serve ad content to different audience segments on internet-based streaming services and internet-enabled TV, based on log-in information, behavior and attributes	●	◑	◑	While the majority of customer audiences are authenticated, shared logins will create issues around precision vs. accuracy. In addition, the impact is dependent on the device (it is higher on desktop, which relies on cookies, and lower on mobile, which is MAID-based)
Activation	Reach and Frequency Capping	Measurement and management of reach and frequency in OTT and CTV against targeted audiences	●	◑	◑	Despite shared logins which create issues around precision vs. accuracy, the authenticated solutions provide will provide a path forward.
Measurement & Attribution	Measurement and Attribution	Overlay Advanced TV exposure data with CRM and purchase data to measure results	◑	○	◑	Attribution in Advanced TV is conducted via "clean" environments synching first party data. While connected TV leverages MAIDs and IP addresses, the identity graph used to connect CRM data to connected TV viewing data still relies on cookies as a foundation. In a post-cookie environment, attribution will be impacted for connected TV due to the loss of precision provided by third party cookie-powered identity graphs

Immature/Low Impact = ○ Maturing/Medium Impact = ◑ Most Mature/High Impact = ●

We expect utilization of these use cases to continue at pace over the next 12–18 months, depending on when Google finishes the deprecation of cookies from its ecosystem—making the last 60% unavailable.

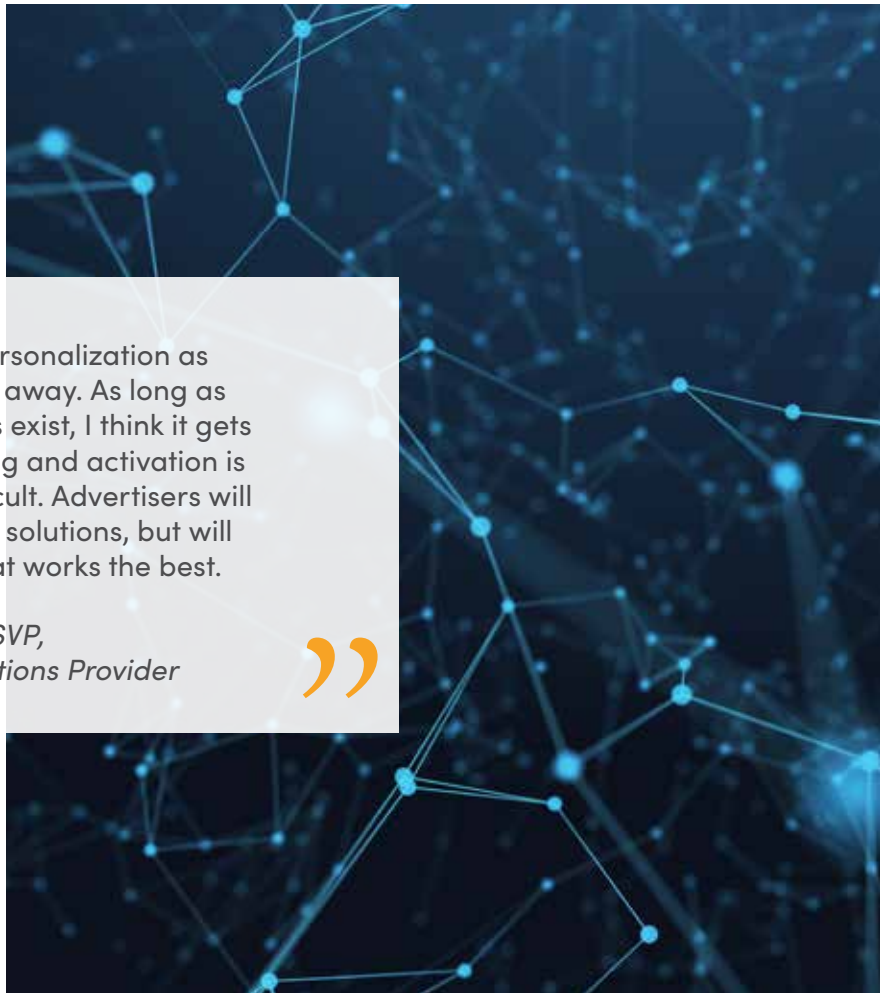
There is some probability, based on comments from the market and pressure on Google from regulators on both sides of the pond, that there could be a delay into 2022. However, for planning purposes, we believe the industry should be ready by the Fall of 2021.

Personalization (on Owned):
Due to its higher maturity and lower regulatory intensity in the U.S., marketing is most likely to be led by the U.S. vendors in U.S. markets.

Programmatic (Paid Digital Media):
We expect that EMEA has the opportunity to lead in creating identity solutions for programmatic efforts, given the head start provided by GDPR. However, it is likely that the U.S. will both adopt and adapt rapidly given its ability to scale investment.

Advanced TV:
ATV is the least mature and most fragmented area in the identity ecosystem. However, ATV and associated identity efforts should evolve in the U.S. market rapidly, especially as COVID-19 applies an accelerant to the shift from linear TV into connected TV.

In order to achieve omnichannel marketing across the complete ecosystem, we believe that the industry will need to begin with orchestration efforts that leverage a common set of identity solutions. But the real obstacle to omnichannel is the silos that exist within organizations and how they use identity to buy and execute media.



> "I don't think personalization as a use case goes away. As long as first-party cookies exist, I think it gets stronger. Targeting and activation is what is more difficult. Advertisers will move to the new solutions, but will have to see what works the best."
>
> *– SVP, Identity Solutions Provider*

REGULATORY IMPLICATIONS & BROWSER RESPONSES

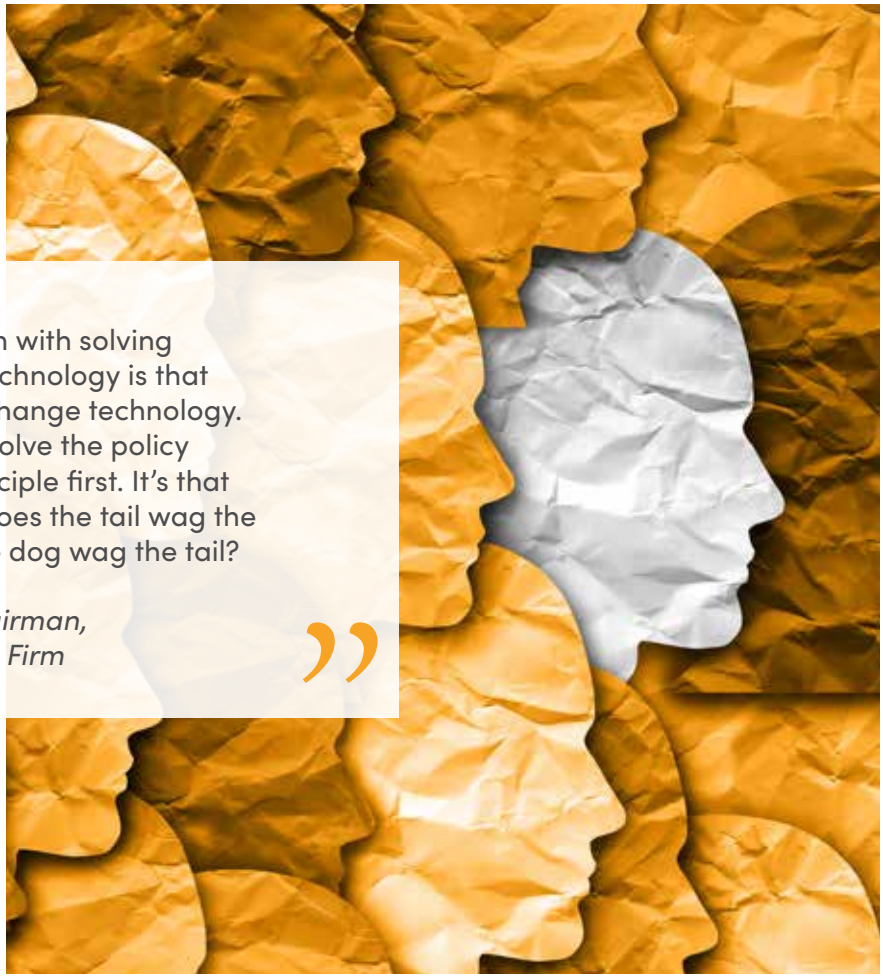
The driving force behind the need to transform the identity landscape is a mixture of "consumer concern," regulatory action and a maturing position of browser owners and other participants. These participants understand that the data they collect is critical to their sustained competitive advantage and that remaining in-step or ahead of both public attitudes and the regulators is a requirement.

The global privacy agenda that has grown around—but generally lagging behind—adtech and martech innovation is a shaping force to the identity solutions that are emerging and will see adoption over the next 36 months.

In our interviews with privacy specialists, the consensus is that **policy will need to be established prior to the industry's ability to clearly define and adopt compliant technical standards**. That being said, there is strong support to move the standards in development through Project Rearc and the W3C whilst policies remain in development.

Part of the challenge that the industry is faced with today is the different approaches to policy embodied within GDPR, CCPA and other U.S. state regulations. There is limited expectation that a common approach to policy will be adopted and therefore the identity market will continue to operate between the constraints of the multiple regimes.

> "The problem with solving identity with technology is that you can always change technology. You have to solve the policy problem on principle first. It's that classic question: does the tail wag the dog? Or does the dog wag the tail?"
>
> *– Chairman, Law Firm*



The key differences between what GDPR wants and what CCPA expects can be summed up in the varying responses to the following five questions:

	GDPR	CCPA	Key Takeaways
What is PII/personal data/personal information?	Personal data is any information that directly or indirectly relates to an identified or identifiable individual.[1]	Personal information comprises information that directly or indirectly relates to or could reasonably be linked to a particular consumer or household.[2] PII is a common wider U.S. term that only includes direct personal identifiers.	The broader the definition of PII, the more likely that attributes that contribute to identifiers will be restricted for use within identity solutions.
Is consent needed?	For digital data: yes for capture and processing for marketing and advertising. Some limited non-consent uses may be available under legitimate interest rules. Postal data can be collected under opt-out rules.	No. An opt out is needed when the data is collected for selling or sharing with a third-party.	The process of acquiring consent and the expansiveness of the notices are increasingly broad in order to retain the ability to leverage data as identifiers.
How long can you hold data?	You can only hold data for long enough to perform the tasks that you stated.	You should hold data for long enough to perform reasonable business activities.	The shorter the period of time that data may be maintained, the greater impairment on the ability to build persistent ID graphs over time.
How can you share data?	For digital data, only with consent of the individual. For non digital data, by opt out.	Only if the individual or household has not opted out via "Do Not Sell".	It's more challenging to build identity graphs with digital data in Europe, while there's limited impairment in the U.S.
What are the permissible uses?	Only in line with what the individual was told at the time of capture.	A wide range of non-credit activities are permitted.	You must have consent in order to use the data for identity.

1 ADAPTED FROM GDPR.EU, 2 ADAPTED FROM COOKIEBOTA

In addition to these key differences, there are several privacy-enhancing concepts that may apply to different identity solution approaches:

Clean Rooms—and a range of associated privacy-enhancing matching techniques—have evolved using the ability to link data via pseudonymization whilst maintaining the security and privacy of that data from both partners. This ability to activate first-party data in another environment without sharing or breaching any of the consumer privacy obligations of either party is a rapidly growing area of activity with use cases across activation, attribution and modelling. This will become a key way that first-party brand owners engage with media owners and their technical partners. Embedded within some clean room approaches is differential privacy, a set of techniques that prevent re-identification and maintain privacy whilst the data remains able to be used for specific purposes. There are initiatives surrounding third-party cookie substitutes that use a differential privacy approach to maintain an open trading currency, but we have yet to see these get mass adoption.

Browsers reject fingerprinting. Aside from the deprecation of third-party cookies, browsers have taken a principle-based approach to safeguarding the privacy of users. All three have stated a rejection of fingerprinting approaches to individual identification and Apple has continued to evolve their rules and policies in response to some companies seeking to find and take advantage of loopholes.

Google's Privacy Sandbox is an evolving set of initiatives aimed at protecting user privacy whilst enabling the advertising industry to take advantage of some information, insight and tools. At this stage, the concept is still in initial phases. However, some key initiatives include 1) all data being held at the device—not server-level—enhancing privacy and negating server-side matching, 2) the provision of a Chrome "conversion management API" for attribution, 3) a "privacy budget" API to restrict data extracted via the browser, 4) the Federated Learning of Cohorts (FLOC) API that uses machine learning to cluster similar behaviors and 5) TURTLEDOVE, a technique for tracking browser interests.

> "There is a group in market that says fingerprinting is a viable solution, but we never have and never will support fingerprinting. Cookies are going away because of the lack of transparency for the consumer, not because the technology was bad."
>
> *– President, Identity Solutions Provider*

The longevity of each identity and targeting approach will depend on potential future changes in the regulatory landscape (in the U.S. and/or the EU), as well as the unpredictability of browsers' policies.

Contextual approaches are primarily immune to these risks given that they do not match any second- or third-party data. Of the approaches with data matching, **second-party clean rooms are the least likely to be affected by regulatory or industry-wide changes** as they maintain first-party data separately and only link anonymous data.

Identity and Targeting Approach	Associated Regulatory and Browser Risk
Proprietary ID based on authenticated first-party data matching	■ Limited browser risk given use of first-party, consented data ■ Requires higher focus on privacy and security of the use and storage of consumers' PII, but holds limited risk in terms of potential future regulations
A common ID based on a first-party data match to a third-party, PII-based reference data set	■ Has browser risk if the browsers decide that the common ID has created a third-party identity workaround ■ Providing that there has been reasonable and fair consent provided, there appears to be limited policy risk
Common pseudonymous ID token	■ Further restrictions around the use of some types of browser or IP signals may limit the ability to fully discriminate
Second-party data environment based on multiple clean rooms with anonymous ID linking	■ Limited browser and policy risk
Household ID based on IP address and geographic match	■ Potential for IP masking by telecom providers and/or browsers introduces some risk to the longevity of this approach, though probably not in the next 24-36 months ■ There is longer term risk in the U.S. that regulatory action may make IP addresses PII, reducing the ability to leverage it as a non-consented identifier
Augmented contextual targeting with segmentation (cohorts) based on first- or third-party data	■ Limited risk at the browser and policy level because this approach leverages contextual information segmented by first-party data
Contextual targeting	■ Limited risk at the browser and policy level because this approach leverages contextual information segmented by first-party datas

Through our interviews, we have identified a number of key considerations that companies that build and/or leverage identity solutions should monitor:

- Our view is that more identifiers will be gradually considered PII within the U.S. system, as initiated by the CCPA. Therefore, it is expected that we will have fewer identifiers available in the future.
- There is an open question as to when MAIDs will follow third-party cookies and be deprecated – their future is in the control of the same browsers who have eliminated third-party cookies.
- IP addresses are already personal data in the EU. In the U.S., it is less likely that it will be considered PII in the short term, largely due to the attribute's role in fraud detection. Device IDs are also personal data in the EU and may face similar scrutiny in the U.S.
- The number of data providers in the EU shrank as a result of both GDPR and local regulation reducing the volume and variety of data available. However, we don't expect shrinkage to the same degree in the U.S., although some will occur due to gaps in policy and sheer scale of U.S. market.

> "I think uncertainty is what's holding people back. In the UK, we saw intelligent brands hit pause because they didn't know what GDPR would mean. As CCPA and other laws come into effect [in the U.S.], it is likely something similar will happen. However, CCPA does bring opportunity."
>
> *– VP of Product, Identity Solutions Provider*

> "The ID needs to decouple itself from a dependency on any other platform ID. First it was cookies, but the writing on the wall says MAIDs will be next as well. Any solution built on a cookie or device ID is unlikely to survive the test of time."
>
> *– Chief Product Officer, Identity Solutions Provider*

MARKET EVOLUTION AND OUTLOOK

What's Next for Identity? As a result of the diversity of requirements across the three ecosystems (personalization, programmatic and ATV) the conclusion that Winterberry Group draws from the market is that multiple identity solutions will be required and continue to evolve in parallel. To achieve the goals of consumer engagement and customer acquisition **marketers will seek to apply a blend of approaches** based on the availability of privacy-compliant identifiers and the suitability of the approach for specific channels and touchpoints.

Publishers and other media owners will also support multiple ID solutions based on their scale of first--party data (and cookies), the audience and geography where their content is consumed and the competitive positioning necessary to compete with the walled gardens. Having lost control of their ability to optimize the monetization of their content and audiences, this evolution away from a third-party cookie paradigm provides the best opportunity to recapture revenue from both subscription and advertising—therefore enabling a more sustainable future. It was clear from our conversations that there is no support for a single ID solution to rule above all others.

Our conversations have also indicated that whilst some technology approaches may span multiple geographic territories, the segmentation of the media industry by language and country indicates that it is **highly probable that identity solutions will see country-level adoption**, with a combination of single publisher ID support and a collaborative model with shared IDs to create scale. Specifically we see this evolving more rapidly within countries across Europe starting in the UK and Germany and expanding across smaller nation states. In this scenario, we expect that the identity solutions utilized will scale across multiple geographies.

> "As a publisher, there's value in first-party data and cookies. It allows us to pull ourselves out of the advertising ecosystem's downward spiral where we feel we are participating in a continuously losing game. [First-party] provides an opportunity to control your own destiny, and there are also more emotional/strategic benefits as well."
>
> *– President, Publisher*

> "There's no perfect future state. The most likely scenario is that people are going to have to be comfortable with multiple methods and methodologies, and then there may need to be human intellectual work applied on top to stitch it all together."
>
> *– Head of Product, Data Services Provider*

Solution Evolution in the Personalization on Owned Ecosystem

As brands seek to elevate consumer experience to drive engagement, loyalty and new customer acquisition, the race is on to scale first-party data assets. This need aligns with the adoption of direct-to-consumer marketing trends and the exponential growth of eCommerce. To achieve these marketing and business objectives, brands are increasingly adopting database management solutions (including those based on CDP technology) with the ability to manage and activate data within the PII and anonymous environment.

For personalization use cases, identity approaches will focus on the resolution of first-party data and first-party cookies that support web- and physical site-based touchpoints. These first-party assets will be deterministically matched when authenticated, with probabilistic matching to increase the ability to recognize across locations and devices.

We expect to see the expanded use of first-party identity graphs over the next 24-36 months, with initial adoption by enterprise marketers, followed by the upper mid-market. Within these first-party identity graphs, privacy-compliant third-party data will continue to be used to enhance and/or enrich the first-party profiles.

The adoption and expansion of first-party identity graphs will increase the availability of deeper analytical approaches, insights and optimization, in addition to providing a foundation to develop collaborative arrangements that leverage clean rooms and other first-party data sharing approaches.

The breadth and availability of first-party data attributes assembled from offline sources and online devices will create the opportunity for advanced machine learning/AI-based decisioning, channel orchestration and customer journey management. In turn, this will create demand for more integrated platforms to support the personalization on owned ecosystems. In addition, a secondary downstream impact of this demand will be an enhanced need for data strategy and services capability within the organization and through partners.

> “I think [cookie deprecation] will force a lot of positive changes. Ripping the Band-Aid off cookie-based infrastructure is ultimately a good thing. For me, it’s even more reason to have a solid ID graph in play. You need user-level data to achieve compliance, to manage user-level permissioning, to manage personalization.”
>
> *– VP, Customer Data Platform*

Solution Evolution in the Programmatic (Digital Media) Ecosystem

The consensus view clearly indicates that the center of the new programmatic ecosystem will also be based on first-party cookies and other first-party data. However, this ecosystem will leverage the broadest set of identity solutions in order to achieve both scale and reach while maintaining the desired level of accuracy (based on use case). Based on our analysis, the five different identity solutions identified earlier in the paper (plus contextual targeting) can be applied to different media offerings based largely on the availability of first-party data, audience volume, frequency of visitation and depth of engagement.

Using the concept of the Walled Garden as the starting point of our framework, we classify these media offerings into four broad groups.

Walled Gardens

Scaled PII (150MM+) High Frequency of impressions, breadth of content, Own their own advertising tech stack, provide limited or no individual data back out, may depend on clean rooms for data ingestion and attribution. Likely to offer private marketplaces.

Examples include Google, Facebook, Amazon, Walmart, TikTok

Private Gardens

Retail and media companies that monetize their inventory and have scaled, authenticated audience, 50MM+ unique visits monthly and/or a very specialized audience, content or product. They either own or license their advertising technology stack and leverage ad exchanges and private marketplaces.. More collaborative with agencies and brands who bring more material spend.

Examples include Xandr, New York Times, Target, Kroger, CVS, Financial Times, WSJ, EA, Epic, Snap, Gannett, Conde Naste, Hearst, Meredith, Disney, AT&T, Sky, Microsoft, Verizon, (CarreFour?, Zalando?)

Communal Gardens

Publisher co-operatives & medium-sized media owners (typically within Comscore 100). Uniqueness of content and/or audience that is likely to have Individual or shared first-party data to enable the creation and distribution of segments,. Greater leverage of probabilistic segmentation. Attribution via clean rooms; data-driven contextual

Examples include Ozone, NetID, Ampersand, Tribune Group, Channel 4, Daily Telegraph, Comscore 100

Rolling Hills

Media owners and publishers with limited scale in first party data and limited unique monthly visits

Examples include specialty publications, news repurposers

As companies grow and achieve greater scale in their first-party data, they can move up this ladder, though it is both difficult and expensive to do so. Media companies that operate within the Advanced TV sector have been consolidating over the past five years, expanding their first-party data assets and facilitating their upward trajectory through the garden types. Additionally, this expansion is enabling them to leverage a broader set of identity approaches.

Premium publishers (private gardens and communal gardens) see the deprecation of third-party cookie as an opportunity to increase their ownership and control of their audience identity. This is leading to the adoption and implementation of reader-first strategies to develop proprietary audiences, increase registration and launch full or partial paywalls—all of which ares designed to expand the scale of their first-party data and cookies.

The characteristics of each garden type dictate the feasibility and likely adoptability of an identity approach. Those with large amounts of first-party data are expected to leverage proprietary or common IDs, while those on the long-tail will need to rely on industry-wide or contextual approaches.

The chart below indicates the propensity of each "garden type" to adopt one or more of the identity solution approaches.

Identity Approach	Walled Gardens	Private Gardens	Communal Gardens	Rolling Hills
Proprietary ID based on authenticated first-party data	●	●	◑	○
Common ID based on first-party data matched to a PII-based reference identity graph	○	●	●	◑
Common identity token used to facilitate enhanced recognition across the pro-grammatic trading ecosystem	○	◑	●	●
Second-party data environment based on multiple clean rooms with anonymous ID linking	○	◑	●	●
Household ID based on IP address and geographic match	◑	●	○	○
Augmented contextual targeting with segmentation (cohorts) based on first- or third-party data	○	●	●	◑
Contextual targeting	◑	●	●	●

Immature/Low Impact = ○ Maturing/Medium Impact = ◑ Most Mature/High Impact = ●

Due to their scale and authenticated approaches, the Walled Gardens can leverage their own proprietary ID solutions—with limited need to extend into the broader set of identity solutions. The market becomes increasingly competitive farther down the "gardens," as advertisers seek similar benefits in accuracy and scale with more control over frequency capping and attribution. We expect that at "private" and "communal" garden levels there will be adoption of multiple identity solutions—and therefore IDs—for each market participant. While we expect the increased use of first-party data-based identity solutions will result in a greater democratization of ad spend across the landscape, we also believe it will significantly expand the complexity in the planning and buying process.

Many industry participants believe the deprecation of third-party cookies could be as impactful on the European marketing ecosystem as GDPR was for the number of third-party data sellers in that region. However, the consensus from the solution providers we spoke to is that the majority of approaches will, in fact, allow third-party data sellers to grow and thrive in the new ecosystem—provided that their data assets are constructed using privacy-by-design.

As a result, Winterberry Group anticipates that third-party data will continue to be used by both sides: for planning and segmentation by the buy side, and for matching and ad delivery by the sell side. We also believe that the emphasis on first-party data in the emerging identity solutions means that there will not be an increase in the percentage of data expense allocated by brands as a percentage of their advertising dollar. Overall, we feel the total amount spent on data and identity will grow in line with the market.

Solution Evolution in Advanced TV

Advanced TV exists within the Communal Gardens ecosystem as result of these providers' ability to generate a combination of individual and household data. The fluid nature of viewing behavior both within the home and outside of it (especially as TV consumption is now portable) provides an expanded set of identity opportunities for targeting and measurement/attribution. However, identity is expected to remain complicated within Advanced TV due to the fragmentation of data origination and control amongst infrastructure, device and content controllers.

In the U.S. market, the continuation of the cord cutting trend coupled with the increase in streaming services is likely to reduce the expected growth rate of linear-based addressable TV. At the same time, the shift away from time-based viewing will provide an increased identity-driven opportunity for more targeted addressable ad insertion. We expect these two forces to ultimately result in greater adoption of identity-driven TV and measurement over time as expenditures shift away from traditional linear programming.

We expect competition for advertising dollars to be split between two programmatic identity approaches: one targeted at the individual and their personal device (and their first-party data) and the second targeted at either the individual or the household on shared devices. Although the in-home TV infrastructure—whether it is tied to a TV set manufacturer (OEM), a set top box controller or a streaming media platform (SMP)—has separate data streams today, we expect that identity solution providers who are building advanced TV identity graphs will provide a bridge between these data environments. Household-based identity targeting will remain the predominant approach in the near term, while hybrid deterministic/probabilistic, individual-device-based models will provide the longer-term solution. If this should happen, we believe that the market will see continued consolidation between programmatic-centric solution providers and TV-centric solution providers.

> "When we talk about ID spaces and Walled Gardens, we need to also talk about the OTT spaces, which are different. Netflix. Hulu. Roku. These are their own semi-closed ID spaces that will become increasingly important as our advertisers see them as strategic and want to shift as quickly as possible to that digital space. But, these identities don't have cookies or Javascript. They need household IDs."
>
> *– CEO, Supply-Side Platform*

> "We believe that identity is a currency within the adtech ecosystem. Knowing a person throughout the lifecycle is of high value. In a way, it is every man for himself—being able to get first-party data is the best way to [manage identity] on your own properties...There are also co-ops working to share information and the industry will see more collaboration. Clean room functionality will also be important."
>
> *– Senior Director, Managed Services Provider*

SIX TAKE AWAYS

First-party identity graphs will need to scale: First-party (private) graphs are critical assets for brands and media owners who seek to compete in an increasingly D2C, privacy-centric, post-cookie landscape. The scale of each graph needs to be appropriate in terms of the coverage and the depth of attributes of each geographic market. Accuracy, however, should be placed at a premium in constructing the graph. The use of partnerships between brands—and between brands and media owners—will enable improved insight, activation and measurement via enhanced scale. However, we anticipate there will be a challenge to not only manage and balance the internal privacy conversation, but also navigate the required investments in technology and data/identity management within a relatively short transformational period before the final deprecation of third-party cookies and potentially other identifiers.

Co-operation is critical to beat the scale of walled gardens: Co-operation is a key part of the future, whether through publishers grouping together to command a larger voice (multi-provider publisher co-ops), media companies and advertisers participating in ID sharing technologies (fully encrypted or merely hashed second-party data agreements between brands and publishers) or new data-first content (ad) networks. In a market that has historically promoted collaboration and coopetition to achieve scale and addressability, the increase in the number of walled gardens (who can deliver on both) will create a push towards more collaboration.

Cohort learning and context will have an important place in the ecosystem: Whilst the use of identity will be a gold standard across the globe, the future will lean more towards "one-to-a few" rather than "one-to-one". The rise of non-personal data sharing and aggregation – FLOC etc. – will attempt to minimize the negatives around this for both advertiser performance and publisher revenue. Emerging contextual solutions will be built with the benefits of recent advances in machine learning and the growth of privacy enhancing edge computing (where user data stays within the device). We believe that media companies who do not have access to identity as a trading currency will be significantly benefited from these emerging developments.

Measurement and attribution becomes harder: Measurement and attribution are going "back to the future" to build insights on a broader canvas of data feeds and identity solutions. MTA solutions will continue to be at the top of marketers' desired data and identity capabilities wish lists; however, the fragmentation across the different types of gardens will remain a challenge. The gaps created by a lack of universal identifiers and the inability to easily collect information from walled gardens are expected to continue. We expect to see ongoing discussion around the use of privacy sandboxes and differential privacy solutions for measurement over the next two years (at least). While MTA will become more challenging, we expect that the deprecation of third-party cookies (with their less than stellar coverage and reliability) will benefit marketers over the long term as new and improved solutions are brought to the market.

Talent gaps, not tech gaps: One of the issues holding the market back is the lack of focus in the brand/agency model that is dedicated to understanding the variety of privacy-compliant identity options. We expect that the increased market complexity in identity will require Chief Data Officers to expand their roles and place themselves at the center of efforts to reduce the media silos that separate paid, earned and owned use cases. The development of talent that overlaps marketing/advertising strategy, data/data science and data privacy will be more critical in the post-cookie, privacy-regulated market than ever before.

A pause on in-housing: In-housing grew in an environment where it became possible to implement a limited number of established tools to manage media. In the emerging market of identity solutions, the need to implement new solutions and manage an increasingly complex media planning and buying process is likely to result in a pause in the shift to in-house models except for the largest enterprise brands. The complexity challenge is reinforced within the CMO's office as the disruption of COVID-19 highlighted the loss of variability in cost management that an in-house solution created. Longer term, we expect that a re-optimization of the blend of in-housing and outsourcing is likely to emerge.

Final Note – Thank you for reading through this exploration of the evolving identity landscape.

Over the next several months as the outlook for advertising and marketing expenditures stabilizes, we will expand on our longer-term forecast and pricing models to align within the evolution of the identity market.

GLOSSARY

Glossary

ANONYMIZATION

The de-identification of data such that it can never be re-identified.

CLEAN ROOMS

Privacy-safe data environments via which platforms, brands and publishers can aggregate first-party user data to expand audiences, gain insights, conduct measurement and determine ad frequency in a secure and privacy-compliant manner. "Safe Haven" is a clean room approach trademarked by LiveRamp.

CONTEXTUAL ADVERTISING

Advertising that uses targeting based on the media content including keywords or whole page topic interpretation through semantic techniques.

CROSS-DEVICE IDENTITY GRAPH

A database of devices that have been deterministically or probabilistically linked based on the available identifiers in order to expand the view of the behaviors of that set of devices, including location. May be linked to an individual or household as part of a third- or first-party graph.

DATA STORE/DATA EXCHANGE

A third-party data store or data exchange is the repository of third-party data placed for license by compilers of third party data (data owners and data brokers), onboarded and matched to cookies and/or other linking identifiers made available to the programmatic marketing ecosystem via DMPs, DSPs, marketing clouds and walled gardens (Google Ads Data Hub, Amazon, Adobe) and data platforms such as Snowflake, among others. The third-party data is segmented and provided for targeting, insights, activation and suppression use cases to advertisers and publishers in the personalization, programmatic and advanced TV ecosystem.

DETERMINISTIC MATCHING

An approach to matching that requires a definitive or exact match of values in two unique pieces of data or identifiers.

DIFFERENTIAL PRIVACY

An approach to eliminating re-identification of data through the addition of extra "noise" formed of incremental, unrelated data. The approach reduces the accuracy of a data set in the effort to gain privacy protection. Typically works best with larger data sets.

EDGE COMPUTING

A computing and storage approach that performs computing efforts near the source of the data (i.e. where the information is produced or consumed, such as connected devices).

FINGERPRINTING

The technique used to identify a device based on monitoring and mapping a wide range of device and other settings.

FIRST-PARTY DATA

Information that is collected directly by the publisher/marketer. Sources of this type of data include information collected from owned properties (desktop, mobile, and print), CRM, email marketing, etc.

FIRST-PARTY COOKIES

Digital tags stored on devices and placed/controlled exclusively by the publisher or brand—used to log user behavior on owned/operated properties. Allow brands/publishers to deliver a more personalized experience, through relevant content and ads.

FIRST-PARTY IDENTITY GRAPH

A database comprised of deterministic, first-party identifiers and attributes (including email addresses, phone numbers, account usernames, etc.) .

GEOLOCATION DATA

Information regarding the physical location emitted from a user's device (mobile, desktop or smart device). The precision of data may vary considerably dependent upon the regulatory regime.

HYBRID APPROACH TO MATCHING

An approach to matching that leverages a sequential combination of both deterministic and probabilistic approaches to optimize accuracy while providing the scale needed to activate desired use cases.

IDENTITY

The effort to recognize and understand individual audience members (including customers, prospects and other visitors) across channels and devices such that brands can interact with those individuals in ways that are relevant, meaningful and supportive of overarching business objectives.

IDENTITY MANAGEMENT

Technology that supports universal user authentication via single sign on techniques.

IDENTITY RESOLUTION

A step in the process of collecting and matching identifiers across devices and touchpoints to build a unified view of an individual customer or prospect that can then be used for segmentation and activation purposes.

IDENTITY SOLUTIONS

The coordinated activation of platforms, data and supporting services (both provided by third parties and sourced from among marketers' in-house resources) that support persistent recognition of audience members across all devices and other promotional and transactional touchpoints.

IFA

Short for "Identity for Advertising, an IFA is used "to maintain a high-quality audience experience within OTT environments [and]

Glossary (continued)

is recommended [for] parties [that] manage advertising related activities" including targeting, frequency capping, fraud detection and reporting.

SOURCE: IAB TECH LAB

MAIDS

Mobile Advertising IDs, or MAIDs, are digital identifiers assigned to a specific mobile device that allow marketers to track, target and attribute across domains. The two most used MAIDs include Apple's IDFA and Google's AAID.

NON-PII DATA

Information that is does not directly identify an individual (or household under CCPA).

PERSONAL DATA (EU)

According to GDPR: "Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

SOURCE: GDPR.EU

PERSONAL INFORMATION (CCPA)

According to CCPA: "Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

SOURCE: CALIFORNIA LEGISLATIVE INFORMATION

PRIVACY-BY-DESIGN

A proactive and preventative approach to privacy intended to incorporate data protection as a grounding principle in the design of data systems, technologies and business practices.

PRIVACY SANDBOX

A solution designed by Google to replace third-party cookies with a range of APIs that rely on signals within a person's Chrome browser. The five APIs include the trust token API, the conversion measurement API, the privacy budget API (which limits the data a website can access through Google), the Federated Learning of Cohorts API (aggregated, cohort-based insights) and TURTLEDOVE.

PROBABILISTIC MATCHING

An approach to matching that establishes a match between sets of data leveraging inferred, modeled or proxy assumptions.

PROFILE

A data asset that ingests and matches identifiers or attributes tied to an individual (and increasingly by household or segment).

PSEUDONYMIZATION

The reversible de-identification of data by substituting data points/characters with pseudonyms using an external key. Pseudonymized data can be linked to other data and thus remains "personal information" under CCPA and "personal data" under GDPR.

REFERENTIAL ID/PERSISTENT ID

An identifier that can be sourced from any combination of consented first-, second- and third-party data that tracks a user across domains and devices.

SECOND-PARTY DATA

A trusted outside organization's first-party data that has been shared primarily to develop consumer insights.

SYNTHETIC IDENTITY

Fabricated credentials where the implied identity is not associated with a real person.

THIRD-PARTY DATA

Data that is collected by a business that doesn't have a direct link to the individual associated with the data.

THIRD-PARTY COOKIE

Digital tags used to understand the behavior of a user across a site or domain which is not controlled by the publisher or brand owner.

THIRD-PARTY IDENTITY GRAPH

A database of profiles built on third-party sourced identifiers and attributes assembled from online and offline sources; data is often linked with first-party data using deterministic or probabilistic techniques.

TURTLEDOVE

An acronym for Two Uncorrelated Requests, Then Locally-Executed Decision On Victory. TURTLEDOVE is a Google-proposed, privacy-safe solution that processes and stores user behaviors locally in their browsers through edge computing (versus the traditional approach of storing these data attributes on s ervers operated by SSPs, ad exchanges or publishers).

ABOUT OUR SPONSORS

Premier Sponsors

Acxiom provides data-driven solutions that enable the world's best marketers to better understand their customers to create better experiences and business growth. A leader in customer data management, identity, and the ethical use of data for more than 50 years, Acxiom now helps thousands of clients and partners around the globe work together to create millions of better customer experiences, every day. Acxiom is a registered trademark of Acxiom LLC and is part of The Interpublic Group of Companies (IPG).

For more information, visit *Acxiom.com*.

LiveRamp is the leading data connectivity platform for the safe and effective use of data. Powered by core identity resolution capabilities and an unparalleled network, LiveRamp enables companies and their partners to better connect, control, and activate data to transform customer experiences and generate more valuable business outcomes. LiveRamp's fully interoperable and neutral infrastructure delivers end-to-end addressability for the world's top brands, agencies, and publishers.

For more information, visit *LiveRamp.com*.

Premier Sponsors

Merkle is a leading data-driven, technology-enabled, global performance marketing agency that specializes in the delivery of unique, personalized customer experiences across platforms and devices. For more than 30 years, Fortune 1000 companies and leading nonprofit organizations have partnered with Merkle to maximize the value of their customer portfolios. The agency's heritage in data, technology, and analytics forms the foundation for its unmatched skills in understanding consumer insights that drive people-based marketing strategies. Its combined strengths in performance media, customer experience, customer relationship management, loyalty, and enterprise marketing technology drive improved marketing results and competitive advantage. With 9,600+ employees, Merkle is headquartered in Columbia, Maryland, with 50+ additional offices throughout the US, EMEA, and APAC. In 2016, the agency joined the Dentsu Aegis Network.

For more information, visit *MerkleInc.com*.

TransUnion is a global information and insights company that makes trust possible in the modern economy. We do this by providing a comprehensive picture of each person so they can be reliably and safely represented in the marketplace. As a result, businesses and consumers can transact with confidence and achieve great things. We call this Information for Good.®

For more information, visit *TransUnion.com*.

Supporting Sponsors

Lotame is the leading provider of data enrichment solutions for global enterprises. Our connected data technologies, curated second-and third-party data exchanges, and high-touch customer service make us the trusted choice for marketers, agencies and media companies that want to build a panoramic view of their customers and activate across the cookieless web, mobile app and OTT environments. Lotame serves its global clients with offices in New York City, Columbia MD, Argentina, London, Mumbai, Singapore and Sydney.

For more information, visit *Lotame.com*.

Neustar is an information services and technology company and a leader in identity resolution providing the data and technology that enables trusted connections between companies and people at the moments that matter most. Neustar offers industry-leading solutions in Marketing, Risk, Communications, Security and Registry that responsibly connect data on people, devices and locations, continuously corroborated through billions of transactions. Neustar serves more than 8,000 clients worldwide, including 60 of the Fortune 100.

For more information, visit *Home.Neustar*.

Tapad, Inc. is a global leader in digital identity resolution. The Tapad Graph™, and its related solutions, provide a transparent, privacy-safe approach connecting brands to consumers through their devices globally. Our one-of-a-kind Graph Select offering enables marketers the flexibility and freedom of choice to correlate devices to varied objectives, driving campaign effectiveness and business results. Tapad is recognized across the industry for its product innovation, workplace culture and talent, and has earned numerous awards including One World Identity's 2019 Top 100 Influencers in Identity Award. Headquartered in New York, Tapad also has offices in Chicago, Denver, London, Oslo and Tokyo.

For more information, visit *Tapad.com*.

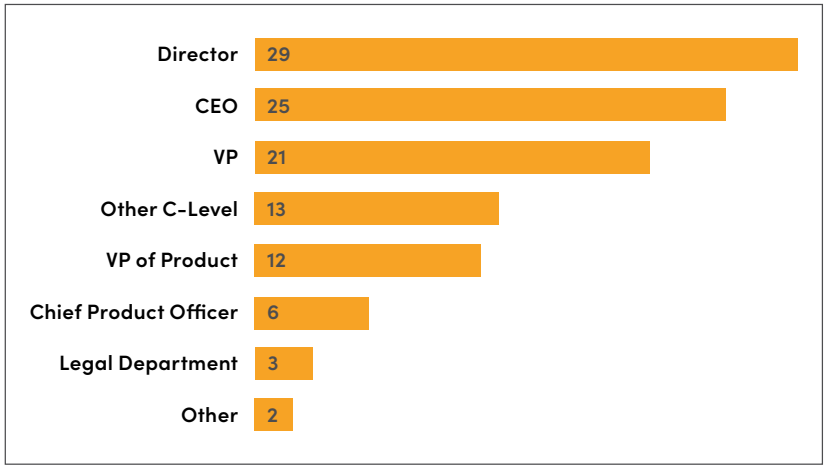
Zeotap is a Customer Intelligence Platform that helps brands better understand their customers and predict behaviors, enabling brands to invest in customer relationships and products that matter.

For more information, visit *Zeotap.com*.

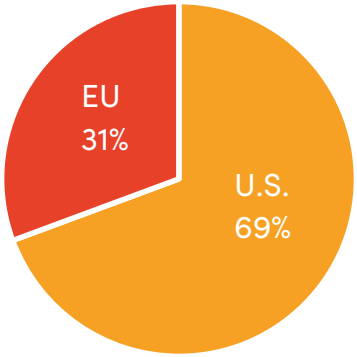
Methodology

The insights in this report were validated by extensive industry research, including off-the-record conversations with some of the industry's top thinkers in the advertising, marketing, publishing, regulatory, legal and agency sectors. We are indebted to the more than 100 individuals who provided their opinions in over 80 hours of video-conference interviews, conducted between March and June 2020.

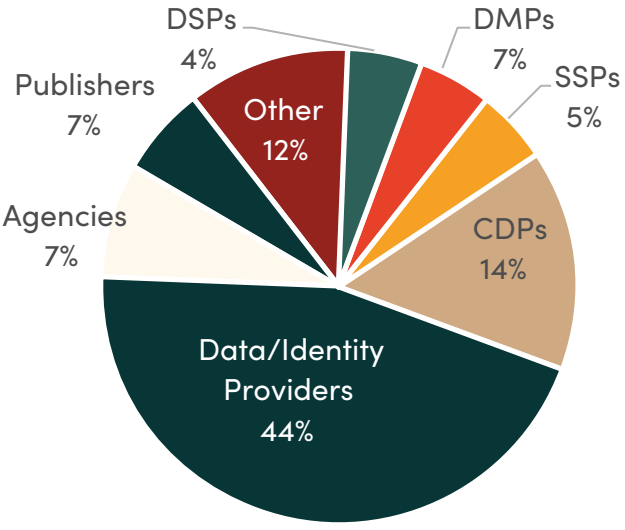
Interviewees, By Job Title (# of interviewees)



Interviewees, By Location (% of interviewees)



Interviewees, By Company Type (% of interviewees)



The companies involved in this effort and to whom we owe our gratitude include:

Acxiom
Adform
Adobe
Alliant Data
Amperity
Ampersand
Analytic Partners
Arm Treasure Data
Axel Springer
BlueConic
Bridg
Bridge
Bristows
BritePool
ComScore
Crimtan
Criteo
Digital Audience
Epsilon
Experian
Eyeota
Flashtalking
FullContact
Google
Havas
ID5
Infosum
Infutor
Kantar
Kinesso
LiveIntent
LiveRamp
Lotame
Lytics
MediaMath
Merkle
MightyHive
Neustar
News Media Alliance
OMD
Oracle
Ozone Project
Permutive
PubMatic
Quaero
Roku
Rubicon Project
Salesforce
Semasio
Semcasting
Sevendata
Tapad
Telegraph Media
theTradeDesk
Throtle
TransUnion
TrueData
Velocidi
Venable
Zeotap
Zeta Global
Zwillgen

About Winterberry Group

A specialized management consultancy that offers more than two decades of experience and deep expertise in the intersecting disciplines of advertising, marketing, data, technology and commerce.

Winterberry Group helps brands, publishers, marketing service providers, technology developers and information companies—plus the financial investors who support these organizations—understand emerging opportunities, create actionable strategies and grow their value and global impact.

Winterberry Group Services

Growth Strategy
Help clients assess core competencies, understand the impact of market dynamics and build actionable, comprehensive strategies that consider a range of "buy, build and partner" opportunities

Digital Transformation
Guide brands and marketing practices through business process planning efforts aimed at helping them achieve lasting competitive advantage—by transforming how they leverage data, technology and digital media

Mergers & Acquisitions
Support investors and operators in their efforts to leverage M&A as a tool for building lasting shareholder value—helping both buyers and sellers better understand addressable market opportunities and dynamics

Market Intelligence
Leverage our independent research platform to help clients and partners achieve clear thought leadership concerning issues of importance to the marketing community

---

Contact Us

Bruce Biegel
Senior Managing Partner
bbiegel@winterberrygroup.com

Michael Harrison
Managing Partner
mharrison@winterberrygroup.com

Charles Ping
Managing Director EMEA
cping@winterberrygroup.com

winterberrygroup.com
115 Broadway, 5th Floor, New York, NY 10006
@WinterberryGrp