ACXIOM POINT OF VIEW

FIRST-PARTY IDENTITY WILL SAVE ONLINE MARKETING

Advertising technology is experiencing a transformation. Having far-reaching effects on consumers, advertisers, publishers and everyone in between, a new baseline is being set, one that will forever change the way these entities connect and exchange value. On center stage is consumer privacy. People have willingly handed over personally identifiable information (PII), like name, email address, physical address, and phone number, in exchange for connectivity with the greater world. Innovation, convenience, and relevant products and services should offer adequate value exchange from publishers and advertisers to "know" or "own" a customer's identity – right? Could it be that the digital transformation happened so fast that the entire ecosystem (including regulators) couldn't keep up?

- What can or should an advertiser or publisher know about you (the consumer) when you haven't explicitly offered consent?
- What "identification" practices should be allowed as brands are looking to reach new customers or provide some form of personalized engagement?

Marketing and advertising technologies have finally reached a pivotal crossroad. Data (specifically PII) has become the new currency, and brands with the most computational power and scalable customer intelligence win. Artificial Intelligence and advancements in device-to-person "resolution" has made possible what once was impossible, scalable identification across the open internet. Yet, major enabling technologies like third-party cookies are under fire and soon are going away. (Some already have.) Rampant fraud and data hacking are driving a backlash of privacy legislation that threatens how brands manage their customers, interact with prospects and analyze their business. All of this is fostering a growing sentiment to own your own data, identity and assets. How did we get here, and where do we go from here?

THE RISE OF THE INTERNET

A lot has happened since the 1990s. Mass adoption of the internet, the invention of smartphones, connected devices, social networks, crowdsourced content (like Yelp) and the direct-to-consumer sharing economy - these have all shifted behavior from a centralized communication model, where conformity was king, to a decentralized and more “open” network, where people can engage with one another and express individual interests and brand experiences. As a result, niche brands have popped up by the thousands across every industry segment. With a treasure trove of behavioral, demographic and geographic data at their disposal, brands were able to precisely reach the right people at the right place and the right time.

Almost overnight, an entirely new advertising ecosystem emerged, built on third-party cookie technology, where advertisers could bid for viewership and quickly measure results per 1000 impressions (CPM), by clicks or by conversions on sophisticated supply-side (publisher) and demand-side (advertiser) ad servers. The martech/adtech landscape also exploded with new entrants and niche players, driving rapid innovation and growth in what “appeared” to be a healthy value exchange. Enter the walled gardens and consumer privacy regulations.

WALLED GARDENS AND THE END OF THE THIRD-PARTY COOKIE

You’ve probably heard the term “walled garden,” referring to the tightly controlled advertising ecosystems that Google, Facebook, Apple and Amazon have built to dominate the internet and modern-day digital commerce. With data privacy at the tip of every regulator’s tongue, these companies have recently announced efforts to raise their walls even higher with the elimination of third-party cookies and mobile advertising IDs (MAIDs), which allowed behavioral tracking and advertising across the open internet.

Google owns 88% of the search engine market[1] and **50% of all browser-based traffic in the U.S.**[2] Meanwhile, **69% of the U.S. adult population regularly consumes Facebook’s content**[3]. The “Big 4” own the devices, browsers, advertising exchanges, the marketplace and the cloud where it’s all stored, moving them ever closer to full vertical integration and the ability to control all aspects of consumer engagement. Many would argue Google is already there. At the center of it all is consumer identity.

So, who are the primary players impacted most by this move away from third-party cookies? The impact is far and wide:

- Independent ad exchanges
- Third-party referential graphs
- Publishers and media owners
- Third-party data aggregators
- Multi-touch attribution players
- Agencies
- Commissioned affiliates
- Brands
- People

Those who are impacted the most are the companies that either built their platforms or justify their value based on distribution and tracking via third-party cookies. Without third-party cookies, many adtech and martech companies are scrambling to reinvent their entire platforms or risk becoming irrelevant. As cookies continue to lose relevance, marketers who want to reach actual customers and serve personalized, meaningful messages must re-evaluate their identity and data collection strategies. Industry regulations are raising the stakes for getting identity wrong and are forcing all players in the garden (walled or not) to take privacy even more seriously.

THE ADVERTISER'S SECRET IS IN FIRST-PARTY DATA

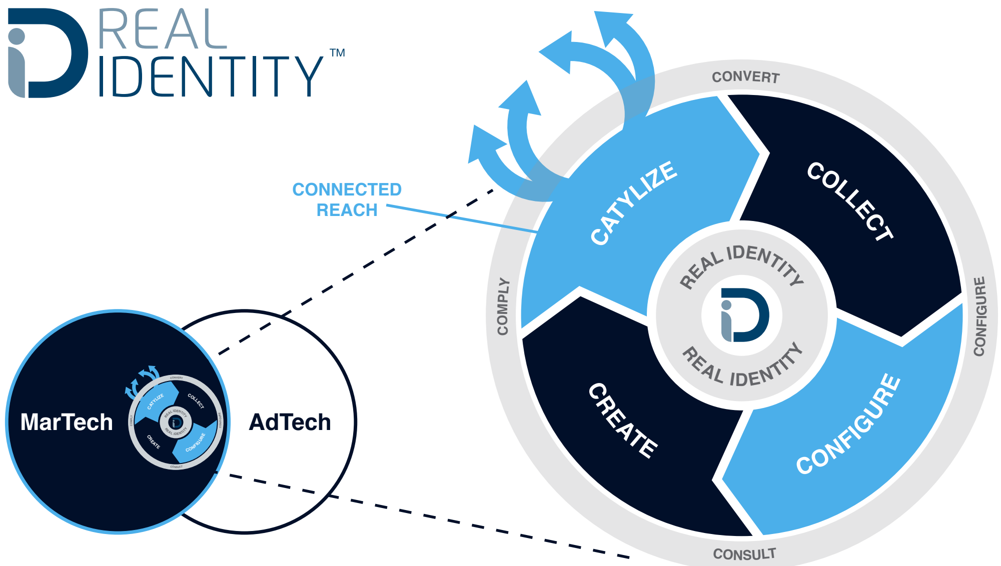
Advertisers must adapt to new and ever-changing customer privacy regulations and take command and control of relationships by focusing on optimization, resolution and enrichment of their "private" first-party data. A brand's data is like a gardener's soil; it's the single most important factor, within the advertiser's control, to grow, nurture and establish positive sustainable relationships with their customers. By getting first-party identity and data management right, the balance between value and privacy is established in the marketing and advertising ecosystem, resulting in meaningful engagements and long-lasting relationships.

Advertisers are now being forced to address the root problem of third-party cookie dependence rather than treat the symptoms. Is there going to be a privacy-compliant and industry-accepted replacement technology? No one really knows. What we do know is that first-party consent-based PII frameworks will play a key role in enabling safe and secure partnerships between advertisers and publishers.

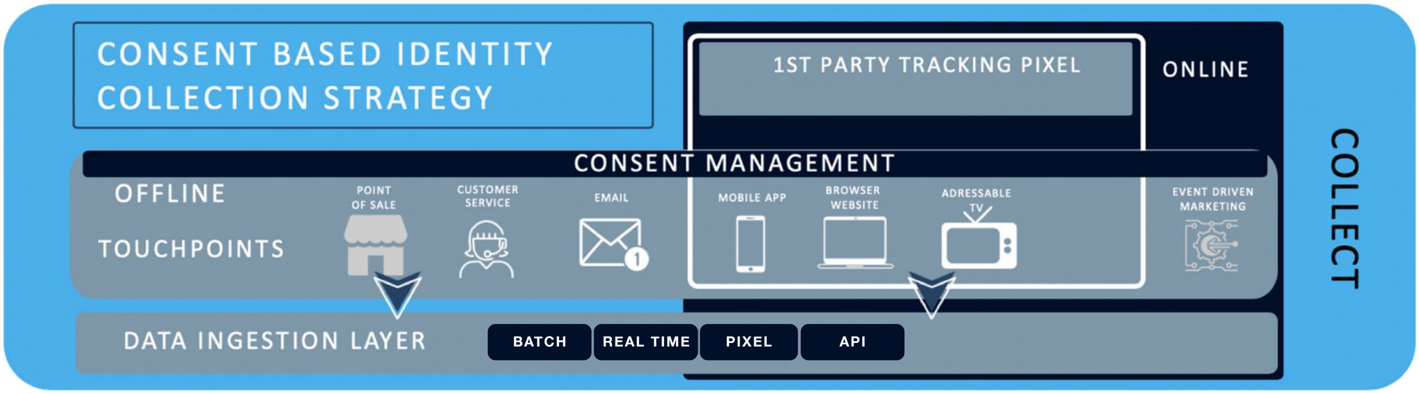
BUILD: Build A Private Identity Graph

The best way to prepare for an unpredictable future is to focus first on what you can control. By building a scalable and configurable private identity graph, you're setting yourself up for success despite constant technology, consumer privacy and vendor changes.

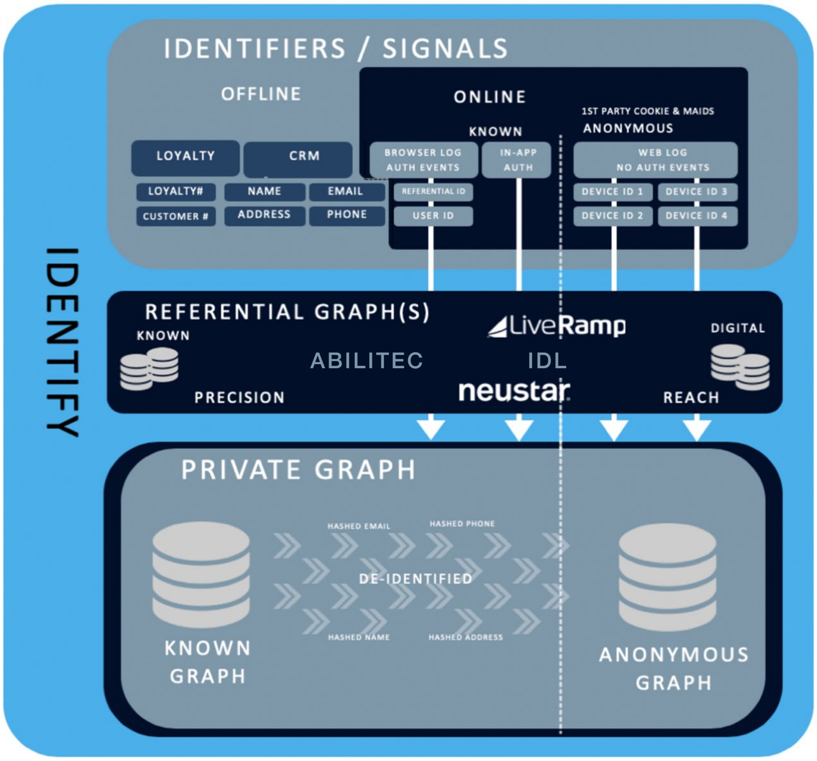
Identity is the cornerstone of any brand's audience or analytics needs, not to mention operational and collaborative use cases, and the list could go on. A brand should use all the data that's available to produce timely and effective identification and consolidation of information to maintain consistent views of entities over time. This includes utilizing a tracking pixel to ingest first-party cookies and MAIDs as a digital extension of a person's channel-less persona. Finally, make sure your graph is tailored to your specific brand and use case needs. No one knows your industry or competitive differentiation like you do. Make sure that differentiation is reflected in your identity graph.



Collect – Incentivize your customers, app users, and website visitors to authenticate. Have the mechanisms in place to capture PII, in the moment, across all channels. Develop an enterprise-wide strategy for increasing authentication across all your online and offline touchpoints. Your ability to talk to people is predicated on your ability to know them. Are you giving your customers or prospects a chance to make themselves known? In return are you incentivizing them with a value exchange for making themselves known?

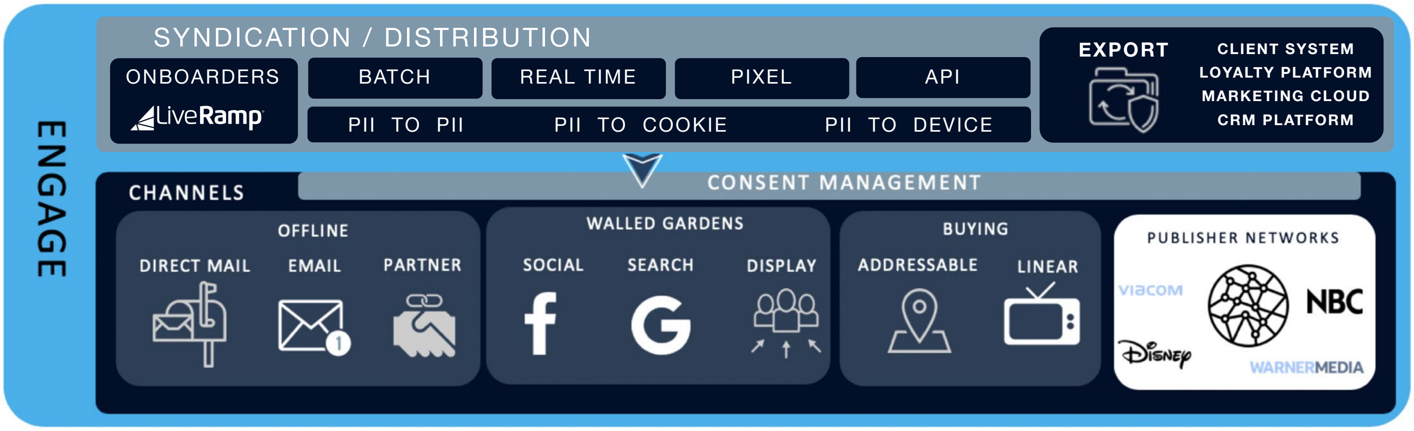


Configure – Every industry, brand and use case is different. Your private identity graph should be tailored to your specific needs. Identity is more than a point-in-time function and is highly influenced by the circumstances and use case. Tuning your private identity graph for the appropriate level of precision is critical for success. Configuring deterministic and probabilistic algorithms to accurately associate identity signals and touchpoints is foundational to delivering the privacy-compliant engagements your customer is expecting. You have to push beyond solutions that focus on a single touchpoint, like hashed email, as the identity spine and configure your graph to take into account all types of touchpoint data to attain a comprehensive view of the customer.



Create – You need to build a privacy-compliant 360-degree view of your customers using a combination of probabilistic and deterministic algorithms. Leverage a historical reference graph providing non-intuitive connections not available in first-party data alone. Manage the changes occurring over time as your customer data changes and relationships between entities split or consolidate. Most brands underestimate the effort of this – it's rather simple to "stitch" data together deterministically; it's another thing altogether to accurately manage life event changes (moves, name changes, device changes, etc.) over time. This is not something most technologies can handle.

Catalyze – Use the single federated key/ID from your private graph as the identity currency throughout your enterprise and as the anchor for translating identifiers for integration with vendor partners and downstream publishers and platforms. The federated key/ID becomes your Rosetta Stone, effectively tying together your martech and adtech stacks . However, identity is of little value if it isn't used to influence your decisions, messaging and offers. Leveraging your private graph to link data and insights to customers and then building and activating audiences is where identity truly delivers value to the enterprise.



Advantages:

- More effective display advertisements that move users through the purchase funnel as well as upsell and cross-sell products and services.
- Improved measurement accuracy so advertisers can better optimize their ad delivery as well as optimize spend across networks and publishers.
- Removed dependency on other third-party vendors for online data ingestion.
- Faster turnaround times for omnichannel identity proofs of concept.
- Audiences anchored in known identities and data.

The Benefits of a Private Identity Graph:

Valuable – You own it. A private identity graph will become one of your brand's greatest assets. Over time, its value will appreciate as it scales and is fine-tuned for accuracy.

Adaptable – As the world around you changes, you need to be able to quickly pivot and adapt to meet your customers where they are, while complying with all privacy standards.

Controllable – As adtech moves to addressable, you can reduce reliance on cookie-based media buying for a significant portion of customer engagements. A first-party graph becomes your "owned" connection into publisher networks and/or second-party partnerships.

Multi-Functional – Identity isn't just about marketing. A first-party private identity graph also ensures your operational use cases, like customer service or internal systems, are kept up to date with all engagements, transactions and touchpoints in real time.

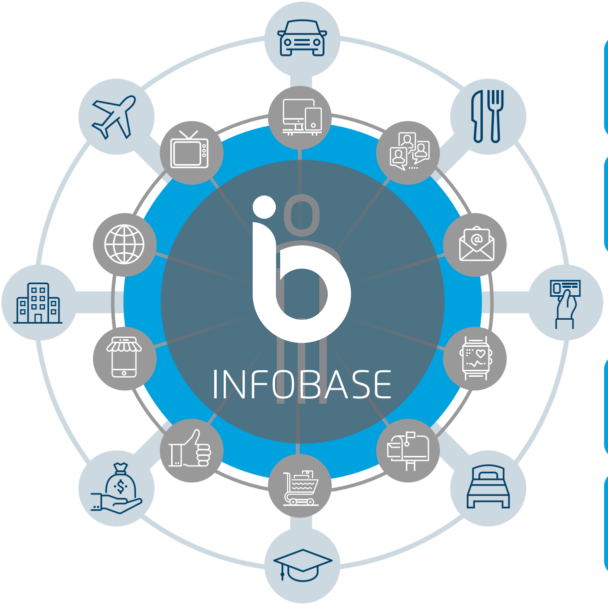
Replace third-party cookies with first-party cookies

Many advertisers have enough site traffic to quickly build a scalable first-party device graph by setting a first-party cookie on their website(s) and app(s). A first-party cookie allows you to analyze and predict browsing behavior while also linking "device-based" identity to a "person-based" identity when someone authenticates on your domain(s). With first-party digital data collection, consent becomes more controllable. Marketing technology companies that specialize in first-party data collection, like Acxiom, are well versed in consent platforms and can provide the gateway to ensure the needs of customers and the ad ecosystem are met. People are finally being given the ability and opportunity to understand what data an advertiser or publisher has about them and request to not be tracked.

WHAT IF YOU DON'T COLLECT FIRST-PARTY DATA?

Take Advantage of Acxiom's PII-Based Data and Insights:

What if a brand doesn't sell directly to consumers? Companies like Coca-Cola and Procter & Gamble aren't collecting PII to build a people-based private identity graph as their business model is selling indirectly through other businesses and service providers. Therefore, they can't deliver personalized ads or find look-a-like audiences using their own first-party data like banks, insurance companies or apparel stores are able to do. Fortunately, Acxiom offers access to the globe's largest ethically sourced demographic and behavioral insights built on a foundation of privacy-compliant and person-based data sources, which can be distributed to a brand's preferred publishers and platforms using direct PII-based connections. With access to thousands of audience selectors, they can leverage Acxiom's audiences for digital and offline engagement for brand awareness or customer acquisition. While campaign measurement and attribution models can be more difficult for non-direct-to-consumer brands, they can still measure engagement and maximize media investments to power more personalized experiences.



260 MILLION US ADULTS

2.5 BN CONNECTED PEOPLE

11,000+ ATTRIBUTES

60+ COUNTRIES

BUILD – at a Glance:

- Collect PII using an enterprise-wide customer authentication and identity collection strategy
- Configure and build your brand-specific private identity graph leveraging a combination of first- and third-party sources
- Catalyze and leverage your federated key into all existing internal and external platforms for audience activation, analytics and operational use cases.

CONNECT: Private Partnerships with Publishers

The days of mass broadcasting are on their way out. Soon, all screens will be connected to the internet and thus "addressable" at the individual or household level. **According to research by Leichtman Research Group, 80% of households have at least one connected TV device**[4].

Nielson's panel data (captured using surveys and panels that consist of a selected group of individuals represented by a sample of the population), has long been the currency publishers have used to inform advertisers of viewership and sell their multi-billion-dollar TV inventory.

The world's largest media brands (e.g. Warner, Disney, NBC, Viacom) are starting to develop their own private gardens (private publisher partnerships) as they already have adequate identity coverage domestically and/or globally. This concept allows them the benefit of monetizing their known high-value audiences and recapturing advertising market share from the walled gardens.

Going forward, most content will be behind a gated login wall or paywall, and people will only be allowed access to premium content if they're willing to make themselves known via an email address, phone number or subscription. This will allow content partners to build up their first-party database and associated customer interests and behaviors.

We will see many advertisers doing direct deals with these publishers, which is how it used to work. Publishers with logged-in users (e.g. Warner's HBO Max and Disney +) will take back lost ad revenue as their inventory becomes addressable (like Facebook and Google). Establishing direct relationships with the right partners will allow advertisers to build on their foundation of first-party data for insights and activation purposes.

Why?

Security – Direct "clean room" matching between advertisers and publishers eliminates the possibilities for leakage and hacking.

Privacy – Consent-based controls will offer people the transparency and ability to opt out.

Precision – PII-based matching and activation will improve engagement, return on ad spend (ROAS) and all advertising KPIs.

Measurement – Direct partnerships will allow you to measure the effectiveness of your media spend.

The Benefits of Private Publisher Partnerships:

Addressable – Media owners are well positioned to take back market share from the walled gardens as new technology is enabling addressable capabilities. As media consumption shifts from linear non-addressable to subscription-based pay walls, brands will have access to scalable direct PII matching.

Measurable – Advertisers will be given full transparency as it relates to impressions, clicks and conversions from ads served within each publisher network.

Permissioned – Regulators are demanding that advertisers and publishers receive explicit consent when using identity services and third-party data for personalization. First-party permissioned PII is becoming the new currency for compliant customer engagement.

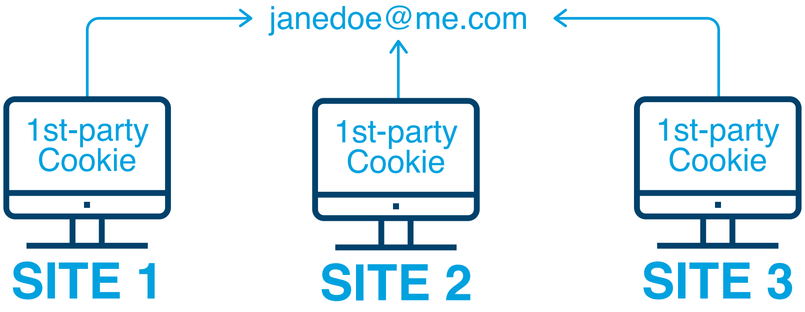
Scalable – The largest publishers (like Warner, Disney, NBC and Viacom) have the domestic coverage necessary to become a viable alternative to existing advertising platforms. Improved ROAS and ad spend efficiency will drive adoption as it did when Facebook first came onto the scene.

CONNECT – at a Glance:

- Identify potential publisher partnerships based on addressable audience coverage and brand relevance.
- Connect via secure and PII-based matching into the publisher networks to ensure no data leakage or privacy risk.
- Measure ROAS compared to existing addressable channels like Facebook and Google.

EXTEND: Leverage New PII-Based Consortiums

New or emerging capabilities, like LiveRamp's Authenticated Traffic Solution (ATS), are being introduced to allow you to contribute to and make use of a PII-based consortium for expanded reach and integration within the programmatic ecosystem (DSPs, SSPs, DMPs). We can assist you in testing their cookieless inventory as a viable long-term alternative to cookies.



Why?

Public – This type of solution allows you to participate in a referential or "public" identity exchange.

Shared "Hashed" Email – Will become the common currency (replacing third-party cookies) in this type of shared ecosystem. This simplifies the "synching" of identity between platforms and drives higher-precision engagements.

Reach – Sharing into a consortium will provide extended PII-based reach across a wider spectrum of advertisers, publishers and content providers.

Digital Personalization – Referential services will extend your ability to retarget site visitors across contributing publisher sites as well as enable site personalization for non-authenticated customers.

The Benefits of PII-Based Consortiums:

Expandable – PII-based consortiums, while in early stages of adoption, are a great way to expand reach into participating SSPs and DSPs while also offering cookieless alternatives for redirecting site visitors across participating publishers.

Trackable – Solutions, like LiveRamp's ATS, are pushing to become the predominant identifier within the existing ad-tech ecosystem. By partnering with DMPs, DSPs, and SSPs, they're able to eliminate drop-off match rates caused by third-party cookie syncs, and reach people within the consortium's cookieless network.

Secure – While you participate in a third-party consortium, ATS ensures no contact information or PII is ever shared with other clients. PII, such as email address, is anonymized in the form of an identity link (IDL) and stored in an encrypted envelope (encoded specifically for your brand).

EXTEND – at a Glance:

- Leverage PII-based consortiums to extend reach and transparency across contributing ad networks
- Qualify and quantify incremental performance compared to existing third-party cookie-based campaigns
- Ensure that proper consent notifications are in place to meet existing or pending regulatory compliance.

And ONE more thing …
THE RESTRICTION of APPLE IDFA (MAID)

In yet another move by one of the walled gardens to further lock down access to digital identity technologies, Apple has announced that it will restrict access to the Apple IDFA (ID for advertising, aka mobile ad ID) in the next major release of iOS. When a person installs iOS 14, which will be available in September 2020, the IDFA will be masked for all apps installed on the device until the app is updated with an explicit consent notification requiring the consumer to opt in to the sharing of the IDFA with the app owner. By effectively "zeroing out" the IDFA by default, advertisers and publishers will lose all ability to identify the unauthenticated user and will no longer be able to provide focused advertising insights.

The move is influenced by several factors, and therefore the impact varies depending on the brand strategy. Currently **Android holds a 3:1 lead over Apple in global OS installation**[6]. In November 2016, mobile market share overtook desktop for the first time and has continued to hold about a 3% advantage[6]. That would seem to diminish the overall impact on a global scale. However, if the advertisers' primary market is the United States, then the tables are turned, with iOS having a 58% to 42% lead over Android[6]. This means advertisers attempting to reach customers in the U.S. market are disproportionately impacted compared to those marketing in other countries.

The other item to consider is that by "zeroing out" the IDFA in all installed apps once the iOS is updated, Apple is further putting iOS-focused advertisers at a disadvantage. **Metrics show that 70% of iOS devices are on the latest version**, indicating that iOS users tend to upgrade regularly. Therefore, there is a high likelihood that **a significant number of iOS devices will be upgrading to the iOS 14 version**[5]**. With more than 1.8 million iOS apps in the Apple App Store**[5], and **1.5 billion active devices**[7], the impact to advertisers is significant.

While this change doesn't mean the IDFA is going away, it does mean brands will initially lose fidelity when it comes to recognizing unauthenticated customers on mobile devices and that people will have more control over what advertisers can or can't know about them. Similar to consent acknowledgement for web-browser tracking, people are much more likely to opt In to IDFA if the application provides adequate value and trust for the identity exchange. This means advertisers will need to be more discerning about which mobile applications they are purchasing inventory for. They will need to focus on apps people find value in and are therefore willing to provide the requisite consent for IDFA access.

CONCLUSION

With all the uncertainty surrounding the end of third-party cookies, ever-changing privacy regulations and new and emerging martech and adtech offerings, our point of view is that a world-class first-party private identity graph, accurately associated with a robust data graph inside a fully integrated and configurable solution framework, is the answer. Despite the end of third-party cookies, taking control of identity across all channels (online and offline) will allow you to master marketing intelligence to make people's experiences better than ever.

Make sure you take time to understand how each of your marketing and advertising technology vendors are preparing for a cookie-less world. For vendors that rely heavily on third-party cookies, make sure you ask quantitative and qualitative questions.

- When will their cookieless capabilities be available for general release?
- What are proven PII-based match rates with supply-side or demand-side platforms?
- Is the new capability being widely adopted by other respected brands in the industry?
- Does this new capability present a potential legal or public relations liability to my brand?

The advertising reformation has only just begun. CCPA and GDPR will certainly be followed by other state, country and industry-level consumer privacy regulations. Emerging players, like CDPs, will continue to push the limits of technological capabilities. Ensure that you're working with a trusted partner to generate success for your business. Take control of your customer relationships by getting identity management right. Acxiom is well versed in leading the world's largest brands through this transformation.

Final Summary:

Build: A Private Identity Graph

Connect: Private Partnerships with Publishers

Extend: Leverage New PII-Based Consortiums

SOURCES

1. https://gs.statcounter.com/search-engine-market-share/all/united-states-of-america#monthly-201901-201912
2. https://gs.statcounter.com/browser-market-share/all/united-states-of-america#monthly-201901-201912-bar
3. https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/
4. https://www.leichtmanresearch.com/80-of-u-s-tv-households-have-at-least-one-connected-tv-device/#:~:text=Among%20those%20with%20any%20connected,2015%2C%20and%208%25%20in%202010
5. https://www.digitaltrends.com/mobile/android-vs-ios/
6. https://gs.statcounter.com/os-market-share/mobile/worldwide
7. https://9to5mac.com/2020/01/28/apple-hits-1-5-billion-active-devices-with-80-of-recent-iphones-and-ipads-running-ios-13/#:~:text=Apple%20hits%201.5%20billion%20active,iPads%20running%20iOS%2013%20%2D%209to5Mac

301 Dave Ward Dr, Conway, AR 72032
acxiom.com
1.888.3acxiom