



The Future of Cookieless Advertising: Adapting to Privacy-Focused Identity Solutions

Abhishek Shetty

abhishek.n.shetty@gmail.com

Abstract As third-party cookies are phased out and privacy regulations become stricter, advertisers face new challenges in targeting and personalization. The advent of privacy-focused identity solutions presents opportunities for adapting to a cookieless future. This paper explores the implications of a cookieless advertising ecosystem, delves into emerging identity solutions, and highlights the strategies businesses must adopt to thrive in this new landscape. By focusing on first-party data, privacy-safe alternatives, and innovative technologies, advertisers can continue to deliver personalized and relevant ads while respecting consumer privacy.

Keywords Cookieless advertising, privacy, first-party data, identity solutions, digital marketing, privacy-focused identity, data privacy, consumer trust, Unified ID, contextual advertising, GDPR, CCPA, consent management, mobile measurement partners, customer segmentation, engagement metrics, cross-device targeting, privacy sandbox.

1. Introduction

The advertising industry is undergoing a profound transformation due to the growing emphasis on privacy and data protection. With regulations such as GDPR and CCPA placing significant restrictions on how advertisers collect and use personal data, reliance on third-party cookies is diminishing rapidly. Third-party cookies, which have been a cornerstone of digital advertising for tracking user activity and enabling personalized ad delivery, are being phased out by major browsers. Google Chrome, which accounts for the majority of global web traffic, has announced the end of third-party cookies by 2023. This shift is part of a broader trend toward protecting consumer privacy and responding to regulatory demands.

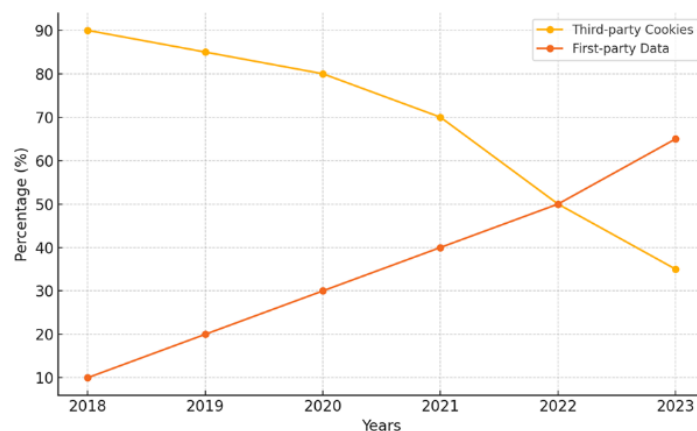


Figure 1: Line graph illustrating the decline of third-party cookies and increased reliance on first-party data (2018-2023)



For marketers, the cookieless future represents both a challenge and an opportunity. Advertisers are forced to rethink their data strategies, focusing on first-party data, contextual advertising, and new privacy-focused identity solutions. As third-party tracking becomes less viable, businesses must learn how to create relevant, personalized experiences while navigating the complex landscape of data privacy.

2. The Demise of Third-Party Cookies

A. The Role of Third-Party Cookies

Third-party cookies have played an integral role in the digital advertising ecosystem since the late 1990s. These cookies allow advertisers to track users across different websites, build detailed profiles based on their browsing behavior, and deliver targeted advertisements that align with user interests. Third-party cookies are instrumental in enabling services like retargeting and cross-site attribution, which are foundational elements of modern digital advertising strategies.

Despite their effectiveness, third-party cookies have become a source of concern for both regulators and consumers. Users often lack transparency regarding how their data is being collected and used, leading to growing distrust of digital marketing practices. Additionally, privacy breaches and data scandals have heightened awareness and prompted stricter regulations.

B. The Shift Toward Privacy

In response to the widespread concerns about privacy, governments worldwide have introduced regulations aimed at giving consumers more control over their personal data. The European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA) are two of the most prominent frameworks designed to protect user privacy by limiting the use of personal data for tracking and advertising purposes.

Browsers have also responded to the demand for privacy. Apple's Safari and Mozilla's Firefox were the first to block third-party cookies by default, followed by Google's Chrome, which will complete its phase-out by 2023. Without third-party cookies, advertisers will no longer be able to track users across multiple websites using traditional methods.



Figure 2: Timeline of browser changes related to third-party cookies (Safari, Firefox, Chrome)

3. Privacy-Focused Identity Solutions

The future of advertising in a cookieless world lies in privacy-focused identity solutions. These solutions are designed to enable advertisers to continue delivering personalized ads while respecting user privacy and complying with data protection regulations. Several alternatives are emerging to replace third-party cookies, each with its own advantages and challenges.

A. First-Party Data

First-party data—information collected directly from users with their consent—has become a critical asset in the post-cookie landscape. Unlike third-party cookies, first-party data is collected by the publisher or advertiser itself, making it a more reliable and privacy-compliant source of user information.



1. Advantages of First-Party Data

O User Consent: First-party data is collected with explicit user consent, ensuring compliance with privacy regulations. Users willingly provide data, making it more transparent and trustworthy.

O Accuracy: Since it is collected directly from users, first-party data tends to be more accurate and relevant than third-party data. Advertisers can use it to gain a deeper understanding of their audience's preferences.

O Ownership: Advertisers have full ownership of their first-party data, allowing them to build direct relationships with consumers and avoid reliance on third-party intermediaries.

2. Challenges of First-Party Data

O Scale: One of the primary challenges with first-party data is its limited scale. Unlike third-party cookies, which track users across multiple sites, first-party data is confined to the advertiser's or publisher's own ecosystem.

O Fragmentation: Advertisers must invest in technologies to unify first-party data across different channels (e.g., web, mobile apps, in-store) to gain a holistic view of the customer.

B. Unified ID Solutions

Unified ID solutions offer an alternative to third-party cookies, enabling tracking without compromising privacy. These solutions rely on deterministic identifiers, such as hashed email addresses or phone numbers, to create a persistent identity for users across websites and devices.

Unified ID 2.0

Unified ID 2.0, an initiative led by The Trade Desk, aims to create a privacy-focused identity framework. By using anonymized email addresses as identifiers, advertisers can track users across sites in a compliant and secure manner.

Benefits:

O Consent-based, privacy-friendly tracking.

O Cross-site targeting remains possible without exposing personally identifiable information (PII).

O Open-source and interoperable with various platforms.

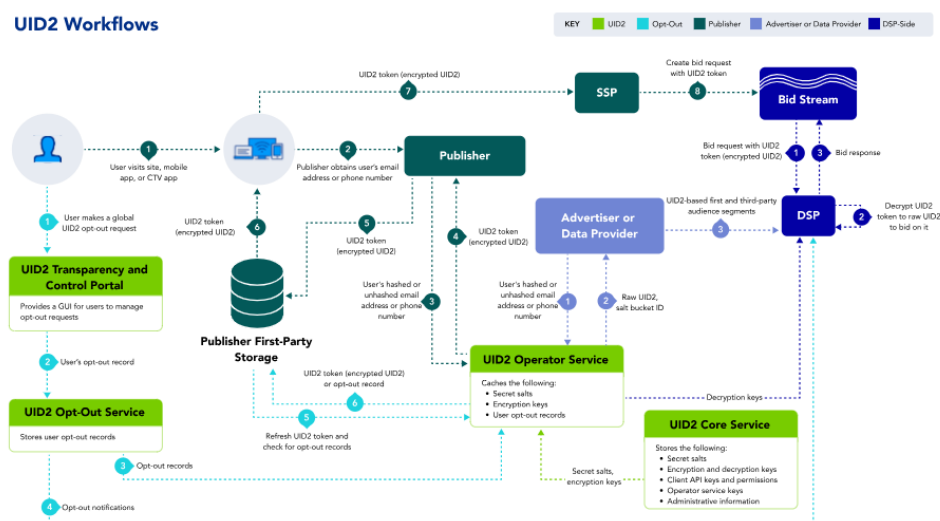


Figure 3: Diagram of how Unified ID 2.0 operates compared to traditional third-party cookie tracking.

C. Additional Identity Solutions

In addition to Unified ID 2.0 and contextual advertising, several other privacy-focused solutions are emerging:

- **Google's Privacy Sandbox:** Google is developing Privacy Sandbox to maintain personalized ad targeting while protecting user privacy. It relies on cohort-based targeting, where individuals are grouped into interest-based categories without exposing personal data.

- **LiveRamp's IdentityLink:** LiveRamp offers an alternative identity resolution platform by matching offline and online data to create unified customer profiles. This approach allows for precise targeting while protecting user identities.



- **FLoC (Federated Learning of Cohorts):** Though discontinued by Google, FLoC was an early attempt at preserving privacy while enabling targeted ads. FLoC grouped users based on browsing behavior without tracking them individually.

D. Contextual Advertising

Contextual advertising is another approach gaining prominence in the cookieless world. Rather than tracking user behavior, contextual advertising delivers ads based on the content of the page the user is currently viewing. For example, an ad for sports gear might appear on a website about fitness or outdoor activities.

1. Advantages

O Privacy-Friendly: Contextual ads do not rely on tracking cookies, making them fully compliant with privacy regulations.

O Relevance: Ads are aligned with the context of the content, increasing the likelihood of user engagement.

2. Challenges

O Lack of Personalization: Since contextual advertising doesn't track past behavior, it lacks the deep personalization offered by behavioral targeting.

4. Adaptation Strategies for Advertisers

With the demise of third-party cookies, advertisers need to adjust their strategies to ensure continued success. Several approaches will help businesses thrive in this new ecosystem:

A. Building a First-Party Data Strategy

In the cookieless future, first-party data becomes a pivotal asset for businesses aiming to maintain personalized experiences for their consumers. A well-structured first-party data strategy allows companies to collect, analyze, and activate data that users willingly share. As third-party cookies phase out, collecting and leveraging this data will enable brands to continue their targeted marketing efforts while adhering to privacy regulations.

1. Prioritizing Consent and Transparency

Collecting first-party data starts with obtaining explicit user consent. Transparency in data collection processes fosters trust and ensures compliance with privacy laws like GDPR and CCPA. Users should be informed about how their data will be used, providing them with clear opt-in choices. Utilizing consent management platforms (CMPs) to give users control over their preferences ensures that your data collection remains compliant.

2. Key Data Collection Channels

First-party data can be sourced from multiple touchpoints where users interact with a business. Here are the most prominent channels for first-party data collection:

- **Website Interactions:** Websites serve as one of the primary hubs for first-party data collection. Tools like Google Analytics enable brands to track user behavior, including page views, clicks, and time spent on site. With Google Analytics, businesses can capture valuable data on user journeys, session durations, and bounce rates, giving them deep insights into consumer behavior. Beyond standard metrics, businesses can employ heatmaps, session recordings, and A/B testing tools to further understand how users engage with different aspects of the website.

- **Mobile Apps:** As mobile usage continues to grow, apps provide direct and rich interactions with users. Mobile app data can reveal user engagement metrics, such as in-app purchases, session duration, and push notification responses. To track and measure app performance, businesses can integrate Mobile Measurement Partners (MMPs) like AppsFlyer, Kochava, or Adjust. These platforms offer attribution and analytics capabilities, allowing businesses to track user behavior, measure the effectiveness of campaigns, and optimize app-based interactions.

- **Email Campaigns:** Email remains one of the most effective channels for first-party data collection. Every opened email, click-through, and conversion can be tracked to understand customer preferences. Through personalized email campaigns, businesses can nurture relationships with existing customers, increasing engagement and loyalty. Businesses can also leverage email sign-up forms to capture essential contact information and segment users based on their engagement with specific email content.

- **SMS Interactions:** SMS marketing provides another valuable channel for collecting first-party data. By encouraging users to opt-in for SMS updates, businesses can engage with their audience directly and track



response rates, click-throughs on SMS links, and engagement levels. With personalized SMS campaigns, companies can offer timely discounts, updates, or surveys to drive customer engagement.

- **Point of Sale (POS) Interactions:** For businesses with brick-and-mortar stores, point of sale systems are crucial for collecting first-party data. Every transaction captures valuable information, such as purchase history, product preferences, and customer details. Businesses can enhance their CRM systems by integrating POS data to provide a holistic view of both online and offline interactions, enabling a seamless omnichannel experience for their customers.

- **Social Media Engagement:** Social media platforms allow businesses to gather a wealth of first-party data based on customer interactions, likes, shares, and comments. By monitoring engagement across platforms like Facebook, Instagram, and LinkedIn, companies can refine their targeting strategies and better understand the types of content that resonate with their audience. This data can be further enriched by monitoring social listening tools to track brand mentions, customer sentiment, and trending topics that are relevant to their industry.

- **Loyalty Programs:** Loyalty programs incentivize customers to share more data in exchange for rewards, discounts, or exclusive offers. By tracking customer purchases and engagement through loyalty programs, businesses can gain deeper insights into their most valuable customers. Beyond simply rewarding repeat business, companies can gather valuable customer feedback through product ratings, reviews, and post-purchase surveys. Moreover, businesses can conduct focus groups and interviews with loyal customers to understand their preferences and improve product offerings.

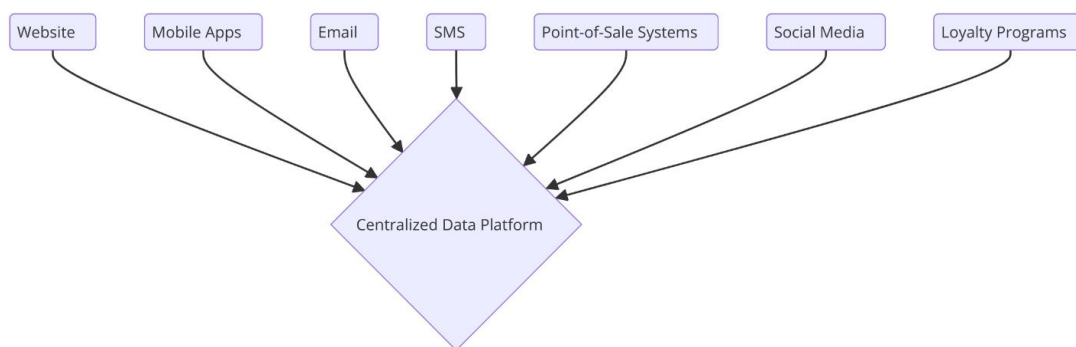


Figure 4: Key channels for first-party data collection feeding into a centralized data platform.

3. Activating First-Party Data

Once first-party data is collected, its true value is unlocked through segmentation and activation. Businesses should focus on creating specific customer segments based on behavior, interests, and demographics to deliver personalized marketing messages. For example, based on past purchasing behavior or browsing habits, brands can personalize email content, app notifications, or product recommendations on their website, making every interaction more relevant and engaging.

The ability to create personalized offers, targeted ads, or customized experiences at scale is key to driving higher engagement rates and improving customer retention. Real-time data activation can also be leveraged to retarget customers, increase upselling and cross-selling, and personalize website content.

4. Data Unification and Integration

One of the most significant challenges in first-party data collection is consolidating data from different channels. To get a comprehensive view of customer behavior, businesses should integrate data sources into a central repository, such as a Data Management Platform (DMP) or Customer Data Platform (CDP). These platforms help unify customer interactions across websites, mobile apps, social media, and offline environments into a single profile. By achieving a unified customer view, brands can create seamless omnichannel experiences and more effectively tailor their marketing strategies.

Integrating data from various sources helps companies eliminate silos, ensuring that data flows across departments (such as sales, marketing, and customer service). This holistic approach enables cross-functional teams to use customer insights for product development, service improvement, and marketing personalization.



5. Enriching First-Party Data with Zero-Party Data

In addition to collecting first-party data, businesses can gather zero-party data, which refers to information that customers willingly and proactively provide. Zero-party data can include details about preferences, intentions, and motivations—information that is not inferred through analytics but is shared directly by the customer. This can be collected via surveys, quizzes, or polls designed to capture more nuanced customer insights. Since this data is voluntarily shared, it provides an even higher level of personalization, allowing businesses to target customers with specific messaging and offers based on their stated preferences.



Figure 5: Differences between zero, first, second- and third-party data

B. Contextual Targeting and Optimization

As the shift away from behavioral targeting takes place, advertisers should focus on optimizing contextual targeting strategies to maintain relevance and user engagement.

1. Content Alignment

Use content relevance to target ads that fit naturally within the environment of the website or app.

2. Advanced Contextual Solutions

New tools, such as Natural Language Processing (NLP), allow advertisers to more accurately analyze webpage content and serve relevant ads.

5. Key Performance Indicators (KPIs) in A Cookieless Future

With the demise of third-party cookies, traditional methods of measuring digital advertising success must evolve. In a cookieless future, advertisers will need to rely on alternative data sources and new metrics to gauge the effectiveness of their campaigns. Below are key performance indicators (KPIs) that can help advertisers measure success in this new landscape:

1. Engagement Metrics

Engagement metrics continue to play a central role in determining the effectiveness of digital advertising campaigns. However, in a cookieless world, there will be greater emphasis on metrics derived from first-party data, contextual relevance, and user-initiated interactions.

- **Time Spent on Page:** This metric measures how long users engage with specific content on owned properties such as websites and mobile apps. Without third-party cookies, advertisers will need to rely on their own analytics tools (e.g., Google Analytics, Mixpanel) to track how long users engage with their content. Longer engagement times can signal higher relevance and interest.

- **Content Interaction:** Metrics like clicks, form submissions, and interactions with interactive elements (such as sliders or quizzes) on a website or app can indicate deeper user involvement. For example, a retailer offering a product quiz on their site can measure how many users engage with the quiz and use that data to tailor future marketing efforts.

2. Privacy Metrics

In the cookieless world, protecting user privacy while delivering personalized experiences will be paramount. To ensure compliance and maintain consumer trust, advertisers should track privacy-related metrics that demonstrate user consent and transparency.



- **Consent Rate:** This metric tracks the percentage of users who consent to data collection on websites or mobile apps. High consent rates indicate user trust and willingness to share personal data for a better user experience. Using Consent Management Platforms (CMPs) ensures that users have control over their data preferences, and advertisers should closely monitor this metric to ensure compliance with privacy regulations like GDPR and CCPA.

- **Opt-In Rate for First-Party Data:** Advertisers should track the percentage of users who voluntarily opt-in to provide first-party data through methods such as account creation, newsletter subscriptions, or loyalty programs. A higher opt-in rate suggests that users find value in sharing their data and are more likely to engage with the brand in the long term.

3. First-Party Data Activation Metrics

As businesses increasingly rely on first-party data, the success of data-driven campaigns will hinge on how effectively that data is activated to create personalized experiences for users.

- **Customer Lifetime Value (CLV):** Measuring the projected revenue a business can generate from a customer throughout their entire relationship with the brand is essential. CLV becomes more important in the cookieless future as businesses need to maximize the value of known customers, rather than constantly chasing new ones through less targeted third-party methods.

- **Personalization Effectiveness:** Advertisers can track the performance of personalized content based on first-party data. This can include metrics such as conversion rate uplift (how personalized messaging affects sales) or engagement rate improvements (how personalized experiences increase interaction).

4. Contextual Targeting Metrics

In the absence of behavioral targeting, contextual targeting plays a significant role in delivering relevant ads without relying on personal data. KPIs specific to contextual targeting can help measure the effectiveness of ads that align with the content users are already consuming.

- **Contextual Relevance Score:** Platforms may offer metrics that score how well an ad fits within the context of the webpage or app where it's being shown. Higher relevance scores generally indicate better ad performance and higher user engagement.

- **Contextual Conversion Rate:** This metric tracks the percentage of users who take action (e.g., make a purchase, sign up for a newsletter) after being shown an ad that's contextually aligned with the content they were viewing. Measuring this provides insights into the effectiveness of contextual targeting strategies.

5. Post-Campaign Privacy Audit Metrics

Advertisers should also ensure that privacy compliance is maintained throughout the lifecycle of a campaign. Post-campaign privacy audits can measure how well user privacy was protected during the campaign.

- **Audit Pass Rate:** This metric shows the percentage of campaigns that passed a privacy audit. A high pass rate indicates strong adherence to privacy protocols, which is critical for maintaining user trust and regulatory compliance.

6. Conclusion

As the digital advertising industry transitions to a cookieless world, businesses must adapt by embracing privacy-first identity solutions and strategies. By building robust first-party data strategies, leveraging unified ID solutions, and adopting contextual advertising, advertisers can maintain personalization and relevance while safeguarding consumer privacy. The future of digital marketing will be defined by how well advertisers can balance privacy concerns with their marketing goals.

References

- [1]. J. Smith, "Adapting to a Cookieless Future: The Role of First-Party Data," *Journal of Digital Marketing Strategies*, vol. 34, no. 2, pp. 112-126, 2021.
- [2]. L. Brown, "Unified ID 2.0 and Privacy-Centric Advertising," *AdTech Insights*, vol. 19, no. 4, pp. 67-80, 2021.
- [3]. K. Roberts, "The Rise of Contextual Advertising in a Post-Cookie World," *Journal of Marketing Innovation*, vol. 11, no. 3, pp. 45-58, 2022.
- [4]. "The Cookie Apocalypse: End of Third-Party Cookies," *DataEQ*, 2021



- [5]. "Unified ID 2.0: An Overview," Unified ID Documentation, 2022
- [6]. M. White, "FLoC: A New Approach to Privacy and Advertising," Advertising Technology Review, vol. 15, no. 2, pp. 98-111, 2022.
- [7]. D. Wilson, "The Role of First-Party Data in Digital Marketing," Marketing Science Quarterly, vol. 28, no. 4, pp. 75-89, 2021.
- [8]. R. Chen, "How Advertisers Can Thrive in a Cookieless Future," Journal of Consumer Behavior, vol. 17, no. 3, pp. 101-117, 2021.
- [9]. A. Lee, "Redefining KPIs in a Privacy-Focused World," Journal of Digital Analytics, vol. 18, no. 3, pp. 55-69, 2022.
- [10]. F. Martinez, "Building Trust with First-Party Data Strategies," Journal of Consumer Trust and Marketing, vol. 29, no. 1, pp. 33-47, 2022.
- [11]. S. Gray, "Google's Privacy Sandbox: A Path Forward," Journal of Advertising Technology, vol. 21, no. 2, pp. 90-102, 2021.
- [12]. P. Johnson, "The Role of LiveRamp in Identity Resolution," Data and Identity Review, vol. 10, no. 4, pp. 48-59, 2021.
- [13]. G. Miller, "Contextual Advertising vs. Behavioral Targeting," Journal of Digital Advertising, vol. 32, no. 1, pp. 67-75, 2021.
- [14]. R. Dawson, "Future-Proofing AdTech with First-Party Data," Digital Marketing Quarterly, vol. 27, no. 3, pp. 83-96, 2022.
- [15]. T. Harris, "The Impact of FLoC on Advertising," Journal of AdTech Research, vol. 24, no. 1, pp. 120-134, 2021.

