White Label Consultancy

Navigating a 3rd-Party Cookie-Free Landscape

March 2024

Table of Contents

1. Introduction

In the current digital environment, where user privacy meets the demands of a personalized online experience, a profound transformation is underway — the gradual phasing out of third-party cookies.

Cookies are small pieces of code that work behind the scenes of targeted advertising, user tracking and seamless web interactions. However, as concerns surrounding privacy and data protection amid technological advancements, major players in the tech industry are ushering in a new era by phasing out these commonly used digital trackers.

This white paper serves as a guide through the shifting terrain of online data dynamics and examines the reasons, challenges, and consequences surrounding the phasing out of third-party cookies.

From their inception as instrumental tools for advertisers to the catalysts behind sweeping changes in user privacy regulations, these pieces of code have played a fundamental role in the evolution of the internet. Consequently, our analysis goes beyond legal considerations and extends into the broader effects felt by businesses, advertisers, and end-users alike.

What does the future look like for personalized advertising? How can businesses adapt their strategies to better align with a digital landscape that values user privacy by moving away from third-party cookies? These are the questions we aim to answer, shedding light on the opportunities and challenges presented by the gradual elimination of third-party cookies.

2. What Are Cookies?

This section introduces key definitions and distinctions crucial for understanding the dynamics of cookies, which will be referenced throughout this document.

A cookie refers to a small text file that a website saves on your device when you visit it. The primary purpose is to help the site remember your preferences (such as username, language, etc.) for a specific duration, eliminating the need to re-enter them during your visit. Additionally, cookies may have other functions like generating statistics to determine the browsing experience on sites.

Types of Cookies: First Party vs. Third Party

Cookies can be categorized along various axes, and one criterion for this classification is whether they are first-party or third-party. This determination is based mainly on their origin.

First party cookies

First-party cookies are exclusive to each website, and only the website itself can access and read these cookies. They are set by the website domain the user is visiting (by the web server or any JavaScript loaded on the website) and are commonly used to collect information that is essential for the website's functionality.

Third-party cookies

Contrary to first-party cookies, third-party cookies rely on information sent by external websites (sent by a third-party server, or sent via code loaded on the website), usually for advertising purposes. These cookies are used to provide personalized information to the user, allowing service providers to deliver targeted advertisements based on the data received. While this enhances ad personalization, it raises considerations about user privacy and data protection.

Are There Any Concerns Related to Third-Party Cookies?

While serving as the driving force behind digital advertising, third-party cookies bring forth numerous challenges. Here, we outline several major concerns associated with third-party cookies, prompting heightened scrutiny and endeavors to tackle privacy issues:

User Tracking and Profiling

Third-party cookies empower companies to monitor users across various websites, facilitating the development of detailed user profiles. This raises privacy concerns about the extensive monitoring of individuals without their explicit understanding or consent, and contributes to a sense of surveillance for the user.

Invasive Targeted Advertising

Advertisers use third-party cookies to deliver targeted ads based on the users' online behaviour. While personalized advertising can be beneficial, the degree of personalization enabled by third-party cookies can feel invasive to users, leading to concerns about privacy and the ethical implications of highly targeted marketing.

Access Control Risks

As data collected by third-party cookies spans across various websites, more entities gain access to it. This, in turn, heightens the risks of unauthorized access or misuse of users' data by malicious parties.

Consent and Transparency Issues

Concerns arise regarding the lack of transparent information and clear consent mechanisms related to third-party cookie tracking. Users may not be fully aware of the extent to which their data is being collected and used for various purposes.

Compliance with Privacy Regulations

Various privacy regulations around the world, such as the General Data Protection Regulation (GDPR) and e-Privacy Directive in the European Union and the California Consumer Privacy Act (CCPA) in California, Saudi's and UAE's Personal Data Laws (PDPL) impose strict requirements on data processing. Third-party cookies often face challenges in meeting these regulatory standards, leading to compliance issues for businesses.

In response to these concerns, there is a growing shift toward exploring alternative technologies and approaches that prioritize user privacy while still allowing for essential functionalities like analytics and advertising. This shift is evident in the development of privacy-focused solutions, as will be discussed in the next section.

3. How Is the Tech Industry Reacting?

Several major players in the tech and browser industry have announced plans to phase out or restrict the use of third-party cookies.

Google

On January 14, 2020, Google announced its intention to phase out support for third-party cookies in its Chrome browser by 2022. This decision was part of Google's broader initiative to enhance user privacy and address concerns about online tracking. The timeline for phasing out third-party cookies by 2022 was set to allow sufficient time for the advertising industry to adapt to the changes. The global resonance of Google's decision underscores a collective desire for transformation within the international market. This impact is particularly noteworthy considering Google Chrome's dominant market share, standing at an influential 64% in web browsing.

In response to this transformative shift, Google has introduced a solution known as the 'Privacy Sandbox,' aiming to establish a harmonious equilibrium between user privacy and the tracking needs of online platforms.

Google's Privacy Sandbox functions like a protected play area, ensuring users' online activities remain private while still enabling advertisers to display relevant ads. Instead of relying on individual data, the system groups people based on their interests, determined by their browsing history. This approach ensures users receive personalized ads without businesses having access to specific details about them.

Apple Safari

Since 2005, Safari has been at the forefront of implementing features designed to curb third-party cookies and cross-site tracking. Notably, the Intelligent Tracking Prevention (ITP) has been introduced gradually through Safari browser updates as a default setting for its users. ITP employs on-device machine learning to identify domains engaged in user tracking, ensuring that the user's browsing history remains private and is not shared with Apple or external servers. Upon discovering domains involved in tracking, ITP promptly isolates and purges any tracking data these domains attempt to store on the user's device.

Mozilla Firefox

Since 2018, Firefox has been committed to bolstering user privacy by announcing its intention to strip cookies and block storage access from third-party tracking content. This commitment then gradually materialized in the form of Enhanced Tracking Protection (ETP), established as the default setting for all Firefox users. ETP functions by blocking third-party cookies and trackers by default, curbing advertisers' ability to track users across different websites.

The system presents users with three distinct levels for managing cookies: standard, strict, and custom. This flexibility allows users to choose their preferred level of privacy for their browsers, with the default setting being 'standard.'

Microsoft Edge

Microsoft Edge includes features like tracking prevention to limit cross-site tracking. While it does not entirely block third-party cookies by

default, it provides users with control over tracking settings.

4. What Are the Negative Effects of Phasing Out Third-Party Cookies?

An experiment conducted by Google investigated the effects of phasing out third-party cookies on publisher revenue. Among the top 500 global publishers, the study uncovered a substantial average reduction of 52% in publisher revenue within the treatment group, where access to third-party cookies was disabled.

These findings are in line with previous academic research. Johnson et al. documented a 52% reduction in revenue from users opting out of online behavioral advertising, and Beales and Eisenach observed that users without cookies generated 37.5% to 66% less revenue compared to those with different cookie settings.

However, the analysis specifically concentrated on primary effects. The removal of third-party cookies could trigger secondary impacts. It may for instance reduce spending by advertising clients due to lower returns on non-personalized ads, and companies may incur additional costs adapting to the challenges of the absence of third-party cookies.

5. Alternatives to Third-Party Cookies

Considering the ongoing trend towards phasing out third-party cookies, companies are compelled to proactively implement strategic measures to navigate this transformative shift in the digital landscape.

This section will explore potential alternatives to third-party cookies, offering companies promising options in lieu of traditional approaches.

Enhanced Conversions

Enhanced Conversions is a Google Ads Tracking feature. The way Enhanced Conversions works is quite simple - when a user interacts with an ad and makes a purchase, that user's data is collected through a conversion tracking tag and sent hashed to Google. It is then used to match against Google data and the account that the user was logged into. According to Google, the first party data is hashed and sent securely. However, hashed data is not anonymous data, so it still should be considered personal data.

For this reason, active user consent is required for valid data processing.

Possible advantages:

Reliance on First-Party Data

Enhanced Conversions concentrates on collecting and analyzing first-party data directly within a specific platform or website.

Improved User Experience

The focus shifts to a more personalized user experience based on on-site interactions. By understanding user behavior within a specific context, businesses can deliver targeted

content and recommendations without relying on extensive external data sources.

Possible drawbacks:

Limited User Control

Browsers and plugins enable blocking and removing cookie data. On the contrary, when hashing data as when using Enhanced Conversions, such data will remain unchanged over time. Specifically, it may persist for many years without any available means for the user to delete it.

Challenges in Attribution Modelling

Enhanced Conversions, by focusing on first-party data within a specific platform, may pose challenges in creating a unified attribution model, making it harder to evaluate the effectiveness of marketing channels accurately.

Potential for Data Silos

Enhanced Conversions rely heavily on first-party data from individual platforms. This can result in data silos, where valuable insights are confined within specific channels or websites.

Device Fingerprinting

Device fingerprinting is a technique for identifying and tracking devices based on their distinctive characteristics or attributes. Unlike cookies, which are stored on a user's device, device fingerprinting relies on collecting information about the device itself, such as its operating system, browser settings, screen resolution, IP address, time zone, installed fonts, and other hardware and software attributes. By combining these attributes, a unique fingerprint or identifier for the device is generated. This identifier serves to recognize the device when it accesses a website, hence allowing it to track user behavior across sites.

Although this might seem as a way to circumvent obtaining the consent that is required for cookies – in the view of Article 29 Working Party, device fingerprinting is not so different and due to accessing data on a user's device, it requires consent when used for tracking users.

Possible advantages:

Cross-Device Identification

Device Fingerprinting does not rely on cookies, making it effective for cross-device tracking and identifying users across multiple platforms.

Improved Accuracy

Device Fingerprinting can offer more accurate tracking compared to cookies, as it considers various device attributes for identification.

Possible drawbacks:

Invasive Tracking

Device fingerprinting can track users across websites without their explicit consent or knowledge. This level of tracking can create comprehensive profiles of users' online behavior and preferences, leading to privacy invasion.

Difficult to Control

Unlike cookies, which users can easily delete or block, device fingerprints are much harder to detect and control. Users might not even be aware that their devices are being fingerprinted, let alone how to prevent it.

Persistent Identification

Device fingerprints are often persistent and difficult to change without altering the device itself. Even if users clear their cookies or use private browsing modes, their devices can still be identified through fingerprinting.

False Positives and Negatives

Device Fingerprinting might not be perfect, leading to both false positives (wrongly identifying two devices as the same) and false negatives (failing to recognize the same device).

AI-driven Contextual Targeting

Contextual targeting is a digital advertising strategy that involves delivering ads to users based on the content of the webpage they are currently viewing. Unlike behavioral targeting, which relies on tracking individuals' online activities and preferences, contextual targeting focuses on the context of the content surrounding the ad placement.

In the modern version of contextual targeting, advertisers, backed by AI algorithms, are fully capable of understanding the nuances of the content, summarizing it, and extracting information. Advertisements are then selected and displayed based on this contextual relevance. For example, if a user is reading an article about travel destinations, contextual targeting might deliver ads related to travel, hotels, or related services.

Possible advantages

Seen as Privacy-Friendly

Contextual targeting focuses on the content being viewed rather than tracking individual user behavior, which can be seen as more privacy-friendly by users.

Content Alignment

Advertisements are aligned with the context of the page, providing a more seamless and less disruptive user experience.

Compliance

Contextual targeting may align better with evolving privacy regulations, as it doesn't rely on extensive user tracking and the need for personal data.

Possible drawbacks

Limited Personalization

Contextual targeting may not provide the same level of personalized ads as behavioral targeting, which could impact the effectiveness of ad campaigns.

Potential Misinterpretation

The context of the content might be misinterpreted, leading to advertisements that may not resonate well with the audience.

Inability to Follow User Intent

Contextual targeting may miss changes in user behavior or intent that are not reflected in the immediate context of the content being viewed.

Topics API

As part of its intention to phase out third-party cookies, Google has over the years proposed new methods for web tracking. It first explored the so-called Federal Learning of Cohorts (FLoC), which was then ruled out for various reasons, including:

Risks of Browser Fingerprinting

FLoC facilitates digital fingerprinting practices by providing a narrower pool of browsers to distinguish from. Instead of having to sift through hundreds of millions of browsers active across the entire internet, advertisers can focus on a much smaller subset within a specific cohort.

Discriminatory Ad Targeting

Since FLoC relies on algorithms to categorize web users, there is a risk that these algorithms may inadvertently reinforce discriminatory patterns present in the data they are trained on.

Potential for Over-Generalization

Cohorts may oversimplify user diversity, leading to potential misinterpretation and over-generalization of user interests or behaviors within a cohort.

Effectiveness in Niche Markets

In niche markets where individual preferences vary widely, FLoC might not be as effective in delivering tailored advertisements.

In response to these criticisms, Google decided to opt out of FLoC in favor of another solution named Topics API. Similar to FLoC, Topics is an interest-based model. As users browse online, the browser will learn about the topics of interest of users without needing to access raw browsing history or personal data. This information is recorded on the user's device and stored for three weeks and then deleted. Furthermore, external parties can have access to a user's topics of interest, but without revealing additional information about the user's browsing activity.

Possible advantages

Exclusion of Sensitive Attributes

Topics are curated to prevent the targeting of users based on sensitive categories.

User Transparency and Control

This technique is designed to be transparent, allowing users to understand the topics assigned to them and potentially change them.

Reduced Tracking Resistance

Since individual user data is not extensively tracked, there is potentially less resistance or pushback from users concerned about online tracking.

Nonetheless, the privacy protections of this second attempt were found insufficient by some.

Possible drawbacks

Risk of Re-identification

In worst-case scenarios, websites could form a hypothesis about the matching of user identities across sites solely based on the data disclosed by the Topics API. However, research conducted by Google suggests that real-world usage tends to align more with the optimistic scenario than the worst-case one. This means that while attackers theoretically could re-identify users across two sites, there might not be computationally feasible attacks to do so.

Competition Asymmetry

Established entities with a history of observing interests gain an advantage by leveraging existing data, while newer or less-established ones may find it challenging to access this information, perpetuating competition disparities.

Accuracy of data

Potential concerns regarding the accuracy and inclusivity of the data, as it may not fully encompass the diverse range of user interests and preferences, especially those belonging to smaller or less mainstream groups.

Server-Side Tracking

Server-side tracking is a method that involves the direct exchange of information between servers, bypassing the need for client-side mechanisms like cookies. Server-side tracking is when a website or an application routes data to your server and then your server relays this data to the destination API or an endpoint.

This method allows businesses to collect data independently of specific third-party services,

such as Google Ads. By setting up their own server-side tracking infrastructure, businesses can gather information about user interactions on their website or app without solely relying on Google Ads or similar services for data collection.

In November 2023, CNIL has also stated that server-side tracking may be a way out when it comes to using Google Analytics and not breaching GDPR rules on data transfers. This is because it is up to the business how to configure the server. It may for instance strip data from identifiers or to hash them, before sending it to third party vendors such as Google Analytics.

It is however worth noting that hashed data may significantly cripple analytics tool used and still do not guarantee full compliance with GDPR rules.

Possible advantages

Enhanced Accuracy
Server-side tracking often provides more accurate data as it eliminates potential discrepancies related to client-side issues or browser settings.

Reduced Dependency on Cookies
Server-to-server tracking is less reliant on cookies, which can be beneficial in scenarios where users frequently clear their cookies or use devices with limited cookie support.

Improved Security
Direct server communication can enhance the security of data exchanges, reducing vulnerabilities associated with client-side tracking.

Possible drawbacks

Complex Implementation
Implementing server-to-server tracking can be more complex and resource-intensive compared to traditional client-side methods, requiring robust server infrastructure.

Limited User Control
Users may have less visibility and control over server-to-server tracking, potentially raising privacy concerns if not implemented transparently. Server-side tracking enables you to track users without them being aware, as they cannot simply access their browser settings to review cookies.

Compatibility Challenges
Server-side tracking may face compatibility challenges, particularly when integrating with diverse platforms and technologies, requiring careful consideration during implementation.

6. Conclusive Remarks

In conclusion, as third-party cookies are being phased out, businesses are compelled to adjust their strategies to harmonize with a digital landscape that places greater emphasis on user privacy.

This white paper provided an introductory glimpse into the nature of third-party cookies, the reasons driving their gradual elimination, and the key players catalyzing this transition. Beyond this exploration, the paper delved into potential alternatives, offering businesses a diverse array of promising options to replace conventional approaches. While the overarching aim was to equip companies with innovative alternatives that could seamlessly replace outdated approaches and foster a more privacy-centric and effective digital landscape, there is a lot of uncertainty regarding how these changes will ultimately manifest and what solutions will prove most effective.

7. How can White Label Consultancy Help?

As the future of third-party cookies remains uncertain, a noticeable shift is underway in the digital landscape. Businesses must proactively stay vigilant and adapt to these changes to ensure the ongoing relevance and effectiveness of their business strategy.

Remaining up to date is not merely a choice but a necessity to safeguard the integrity of business strategies. Adapting to the evolving digital environment ensures that companies can maintain a competitive edge and effectively engage with their audience in a privacy-centered era.

White Label Consultancy allows you to put your privacy compliance and organization's reputation into the safe hands of experienced and senior privacy professionals. Being a boutique data protection and privacy consultancy with highly specialized privacy professionals, White Label Consultancy has vast experience implementing privacy management programs across several large multi-nationals, working in both in-house and consultancy roles.

We combine excellent legal proficiency with deep technical knowledge and significant operational experience to offer a made-to-measure, proven, and functional approach to solving the issues that organizations face.

Each organization is different, but WLC offering can be tailored to the needs of the organization, both in terms of support offered and the time allocated.

Conclusive Assessment

Technology	Involves PII?	Tracks Individually?	How does it track users?	Degree of control over data (business perspective)	Steps needed to comply with GDPR	Steps needed to comply with ePrivacy	Overall privacy friendliness
Third-Party Cookies	Yes	Yes	Third-party cookies are dropped via a specific vendor code or tag deployed on a particular website and stored under a different domain. Data from cookies are used to build users' profiles and adjust ads to their preferences and interests.	Low/Moderate	Requires notice, consent, CMT	Requires notice, consent, CMT	Low
Enhanced Conversions	Yes	Yes	Matches hashed 1st party conversion data from a website against data possessed by Google	Moderate	Requires notice, consent, CMT	Requires notice, consent, CMT	Moderate
Device Fingerprinting	Yes	Yes	Creates a UserID based on different variables from the user terminal to build a user profile and personalize ads.	Low	Requires notice, consent, CMT	Requires notice, consent, CMT	Low
AI-driven Contextual Advertising	No	No	It does not track users directly. The content of the website is analyzed and used to suggest an ad to the user.	N/A	N/A	N/A	High
Topics API	Yes	Yes	The browser identifies the user's primary browsing interests weekly and clusters them into topics on the device without external server involvement. When the user visits a website, the Topics API shares three selected topics from their browsing history with the site and its advertising partners.	Moderate	Requires notice, consent, CMT	Requires notice, consent, CMT	Moderate
Server-side Tracking	Yes	Yes	It assigns an identifier to website visitors when they interact with a webpage by clicking a link, submitting a form, or browsing a page. This identifier is stored on a private server and may be shared with publishers' servers for marketing purposes.	High	Requires notice, consent, CMT	Requires notice, consent, CMT	Moderate

Authors

Nicholai Pfeiffer

Managing Partner

White Label Consultancy

np@whitelabelconsultancy.com

Dr. Magdalena Góralczyk

Data Protection Partner

White Label Consultancy

mg@whitelabelconsultancy.com

Przemysław Gruchała

Senior Consultant

White Label Consultancy

pgr@whitelabelconsultancy.com

Lucrezia Nicosia

Associate

White Label Consultancy

lni@whitelabelconsultancy.com

Contact

hello@whitelabelconsultancy.com
+45 71 74 74 54

NORWAY

Main Office Oslo

+47 4141 2168

Fjordalléen 16
0250 Oslo

DENMARK

Copenhagen Office

+45 71 74 74 65

Dampfærgevej 27
2100 København Ø

POLAND

Warsaw Office

+48 515 07 99 77

Ul. Marszałkowska 58/15
00-545 Warszawa

UNITED ARAB EMIRATES

Dubai Office

+971 50 4536616

Dubai World Trade Center
Dubai

WHITELABELCONSULTANCY.COM