DATABEAT

WHITEPAPER

Surviving the Post Cookie Era

Adapting to the Future of Digital Advertising

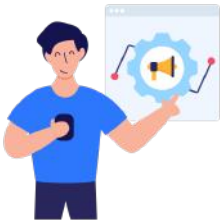
About DataBeat

DataBeat is a trusted partner to publishers, SSPs and various agents in the Ad Tech space. We employ the best minds on your business to make the most of your data, augmented by our analytical capabilities.

Our experts aim to deliver state of the art in strategy, product and personalized innovations for you to keep up with the ever-changing conditions of the digital advertising space.

Yield Analytics

Engineering Services



Campaign Management

Advanced Analytics

Data and Analytics Strategy and Architecture

Custom Development and Visualization

Get in touch

ashok@databeat.io
Ashok Ganapam
CEO
www.databeat.io

DATABEAT

Table of Content

DATABEAT

Overview

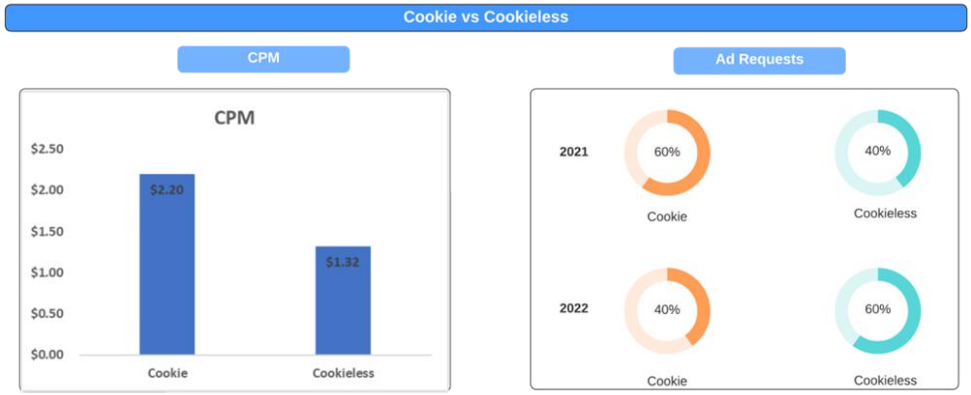
In January 2020, Google announced that they will stop supporting third-party cookies in Chrome by 2022. However, they recently moved the deadline to early 2023. This has the potential to change the landscape of digital advertising, which currently relies heavily on third-party cookie data for personalization.

As a result, companies must prepare for and adapt to the new changes in personalization solutions.

Although the new deadline may seem far away, time flies, and Companies still have a lot of preliminary work to do. The ban on third-party cookies will have a massive impact on the digital advertising landscape, and it may even be a topic of discussion for the rest of the decade.

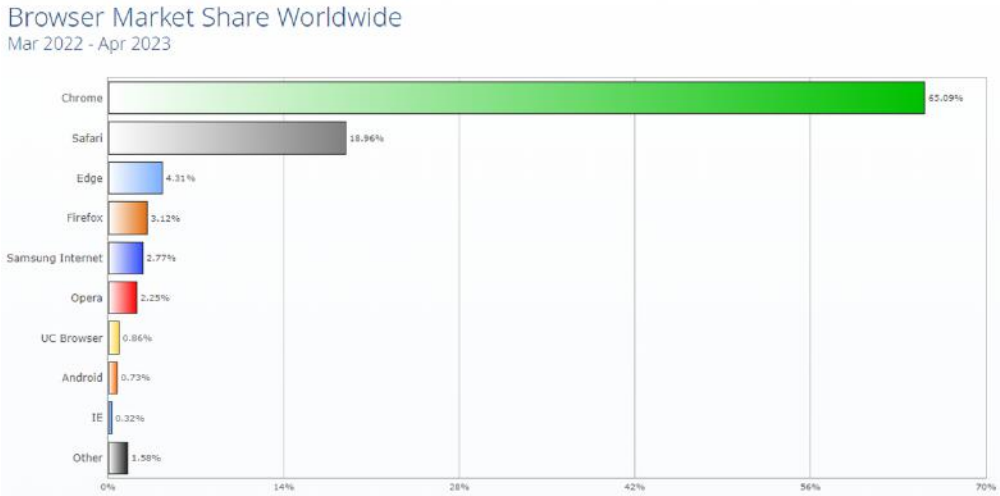
Decline in Cookie Match Rate for Publishers

As cookie match rate is dropping over the years. Because of this change, SSPs see a drop-in bid rate, CPMs, and Spend from DSPs. Due to this many publishers are seeing a drop in CPM's/revenue from some of the SSPs and publishers might see a 40% drop in CPM in the cookieless world.



Browser Market Share Worldwide

With the industry showing that 65% of users are primarily on chrome, any changes to the chrome environment will have to be closely monitored by all stakeholders in the field to ensure that they are able to find alternatives to cookie based targeting.



DATBEAT

What are cookies?

Cookies are small text files that a website sends to a user's browser and are stored on the user's device. They can be used to remember user preferences, login information, and other data that helps improve the user experience.

How are cookies collected from users?

Cookies are collected in various ways as shown below

Type of Cookie	Description	Example
Zero-Party Cookies	Cookies that are created and used by the website a user is visiting	A website might use zero-party cookies to remember a user's language preference or shopping cart contents.
First-Party Cookies	Cookies that are created by the website a user is visiting and are used to enhance the user's experience on that website	A news website might use first-party cookies to remember a user's login status or to save a user's preferences for the website's layout.
Second-Party Cookies	Cookies that are created by a website other than the one a user is visiting and are used to collect data on behalf of that website	A marketing company might use second-party cookies to track a user's browsing history on a particular website and then use that data to display targeted ads.
Third-Party Cookies	Cookies that are created by a domain other than the one a user is visiting and are used to track a user's browsing behavior across multiple websites	Advertising networks often use third-party cookies to track a user's interests and display targeted ads across different websites.

ZERO-PARTY	FIRST-PARTY	SECOND-PARTY	THIRD-PARTY
Consumer intentionally provides	Business collects via consumer's interaction with its properties	Another business's first-party data you use with formal permission	Aggregated info strung together from public and non-public sources
Self-reported			
Direct relationship, not shared		**Indirect, shared**	
Individual data, consented, low volume, high accuracy			**Aggregated, consent varies, high volume, low accuracy**
Product preferences	Purchase history	Fashion brand purchase data sold to a CC company	Purchases from sites across the web

DATABEAT

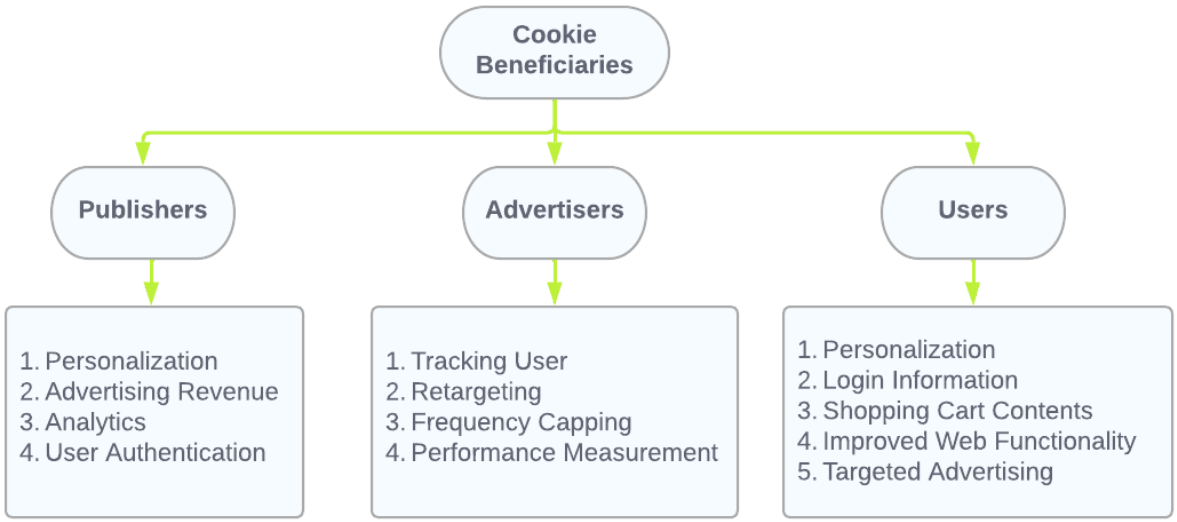
Stakeholders Who Benefit from Cookies

- **Website owners / Publishers**: Cookies can help website owners track user preferences and behavior, which can be used to improve the user experience, personalize content, and target advertising.

- **Advertisers**: Cookies can help advertisers track user behavior and interests, which can be used to serve targeted ads that are more relevant to the user.

- **Users**: Cookies can make it easier for users to navigate websites and remember their preferences, such as login information, language preferences, and shopping cart contents.

- **Web developers**: Cookies can be used by web developers to store user data, such as form submissions and preferences, and make websites more interactive and functional.



DATABEAT

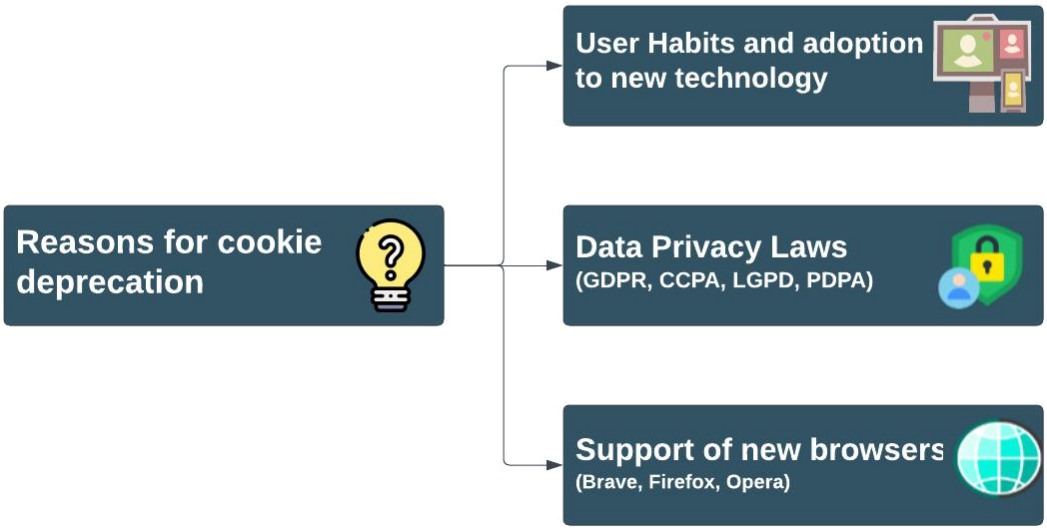
Cookie Deprecation: Drivers and Consequences

- The use of cookies is not likely to be completely deprecated, as they are an important tool for website functionality and personalization. However, there has been increasing concern about the privacy implications of cookies and how they are used by advertisers and other third parties.

- Some web browsers, such as Safari and Firefox, have taken steps to limit the use of cookies by blocking third-party cookies by default. Google Chrome has also announced plans to phase out support for third-party cookies in the near future, although it is expected that some form of cookie-like technology will still be used.

- There are also alternative technologies being developed that could replace cookies, such as browser fingerprinting and server-side tracking, which are less reliant on storing data on the user's device. However, these technologies are still in the early stages of development and may not be as effective or reliable as cookies in all use cases.

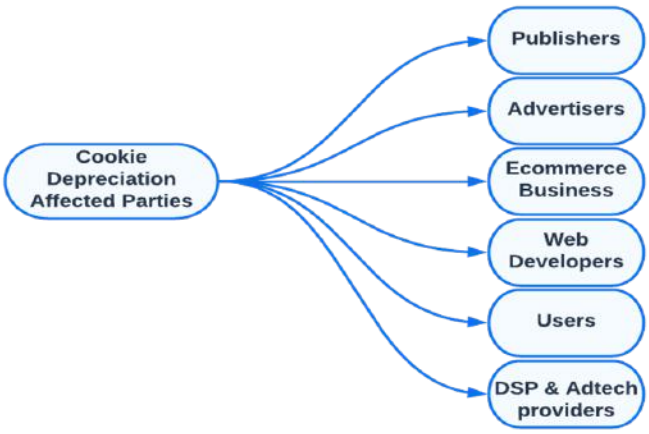
- Overall, while cookies are not likely to be completely deprecated, there is a growing trend towards limiting their use and exploring alternative technologies that offer greater privacy and security for users.



DATABEAT

Impact of Cookie Deprecation: Identifying Affected Parties

- **Advertisers**: Advertisers who rely on cookies for tracking user behavior and serving targeted ads may need to find alternative methods to gather user data and deliver personalized advertising.
- **Publishers**: Publishers who rely on advertising revenue may see changes in how ads are served and targeted, which could impact their revenue.
- **E-commerce businesses**: E-commerce businesses that use cookies to track user behavior and personalize the shopping experience may need to find alternative methods to gather user data and provide a personalized experience.
- **Web developers**: Web developers who rely on cookies for website functionality and analytics may need to find alternative methods to track user behavior and gather data.
- **Users**: Users may see changes in how their data is collected and used by websites, and may need to adjust their cookie settings or preferences to ensure their privacy is protected.
- **DSPs & Adtech Providers**: DSP vendors need to revise their strategies due to the threat posed by media giants such as Google and Facebook, who offer their first-party audiences for free. DSPs still provide granular targeting and campaign management through other parameters, and access to inventory through partnering ad exchanges for display and video advertising. Other ad tech or ad buying solution providers, such as social platforms, will also need to adapt their standard tactics on collecting user data without the use of cookies. It is unclear what the implications of the third-party cookie bans will be for 'cookie piggybacking' or other indirect ways of transferring first-party cookie data usually practiced for ad serving.

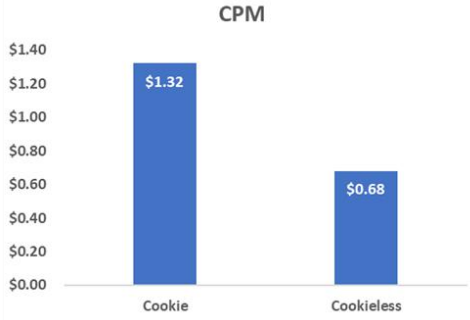


The Adverse Impact of Cookie Deprecation on Publishers

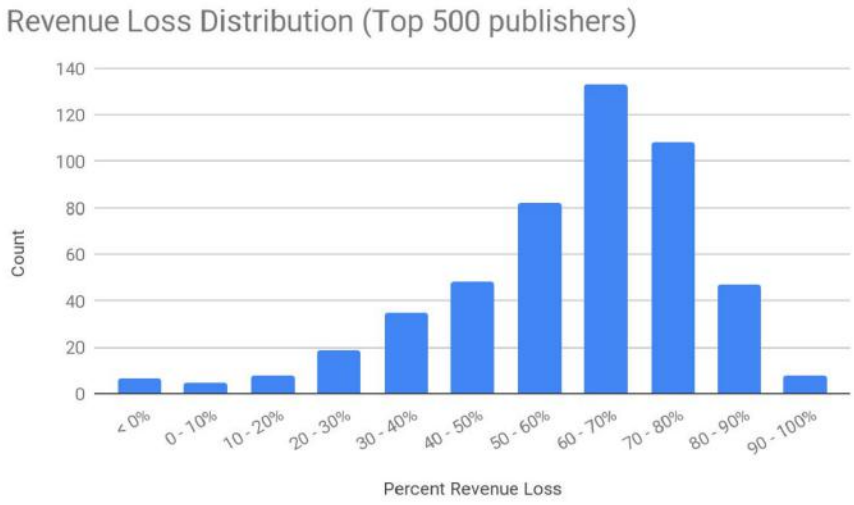
Loss of Revenue: Publishers may experience a significant drop in revenue (up to 45% decrease in CPM) without third-party cookies for targeted advertising.

Below are the main factors causing it

- **Reduced Targeting**: Removal of third-party cookies could decrease ad spend and revenue for publishers, especially those relying on programmatic advertising, due to the difficulty of targeting specific audiences.
- **Loss of Data**: Publishers may lose valuable user data previously collected through third-party cookies, which could impact their content and advertising strategies.
- **Ad Fraud**: Without third-party cookies, it could become easier for fraudsters to spoof user data and generate fake ad impressions, leading to a decrease in advertiser trust and revenue for publishers.
- **Increased Costs**: Publishers may need to invest in new technologies and strategies to adapt to a cookieless web, which could be costly and time-consuming.



According to a Google study on the impact of cookieless targeting, the top 500 global ad publishers saw a 52 percent drop in ad income.



The Adverse Impact of Cookie Deprecation on Advertisers

- **Reduced Targeting**: Without the use of third-party cookies, advertisers will have a harder time targeting specific audiences across the web. This could lead to decreased ad effectiveness and lower ROI on advertising spend.
- **Loss of Attribution**: Third-party cookies track conversions and attribute them to campaigns, making it harder for advertisers to measure success and optimize strategies without this data.
- **Increased Costs**: Advertisers may need to invest in new technologies and strategies to adapt to a cookieless web, which could be costly and time-consuming.
- **Decreased Scale**: Without the ability to track users across the web, the scale of available audience data could decrease. This could lead to decreased reach and lower ad effectiveness.
- **Difficulty in Frequency Capping**: Without cookies, advertisers will have a harder time controlling the number of times an ad is shown to a user, potentially leading to ad fatigue and decreased ad effectiveness.

The Adverse Impact of Cookie Deprecation on Users

- **Reduced personalization:** Without the use of cookies, websites may not be able to provide a personalized user experience based on previous user behavior and preferences. This could result in less relevant content and recommendations being presented to users.
- **Reduced convenience:** Not storing information in a cookie can lead to manual entry of login details and preferences, which is inconvenient and time-consuming.
- **Limited access:** Some websites or web applications may not function as intended without the use of cookies, so users may need to adjust their browser settings or use alternative technologies to access certain content or services.
- **Less effective advertising:** Depreciating cookies may reduce personal data collected for ads, resulting in less effective and less targeted advertising to user's interests.
- **Increased complexity:** The shift away from cookies may lead to the development of new technologies and methods for personalization and user tracking, which could result in increased complexity and uncertainty for users

The Benefits of Cookie Deprecation to Users

- **Enhanced security:** The depreciation of cookies can enhance user security and privacy by limiting the amount of data stored and shared with third-party websites, reducing the risk of sensitive user data being stored on devices and exposed to cyber threats.

- **Tracking:** Users may have more control over their online tracking preferences and the data that is collected about them. This could mean fewer targeted ads, but also less invasive tracking of their online behavior.

- **Improved privacy:** Cookies are often used to track user behavior across the web, and the depreciation of cookies is expected to limit this tracking, providing users with greater privacy.

- **Less invasive advertising:** Cookies are often used to serve targeted ads, which can be perceived as invasive by some users. The depreciation of cookies is expected to reduce the amount of personal data that is collected for advertising purposes and provide a less intrusive ad experience.

- **User control:** The depreciation of cookies is expected to give users greater control over their online tracking preferences and the data that is collected about them.

What does the Future look like without Cookies?

A future without cookies would change online advertising and marketing significantly. Advertisers and marketers would need to find new ways to target and personalize messaging to consumers, potentially through contextual advertising, behavioural targeting or first-party data collection.

However, this may also have implications for user privacy, as it could be more difficult to control data collection and prevent malicious activity. The future without cookies is likely to require new approaches to online advertising and be more privacy-focused.

Degree of reliance on third-party cookies in digital advertising in the US

Surviving in a Cookieless Environment: Alternative Approaches

1. First-party data collection

First-party data collection is the process of gathering information directly from your customers or users, typically through their interactions with your website, mobile app, or other digital channels. This data is owned and controlled by you, the first-party, and can be used to better understand your customers' behavior and preferences, as well as to improve your marketing and advertising efforts.

Here are some common ways that companies collect first-party data:

Website analytics: Companies use website analytics tools, such as Google Analytics, to track user behavior on their website, including page views, clicks, and time spent on site.

Customer relationship management (CRM) data: Companies use CRM systems to manage customer interactions and transactions, including contact information, purchase history, and customer service interactions.

Email marketing: Companies collect email addresses through opt-ins and sign-ups for email newsletters, promotions, and other marketing campaigns.

Mobile app usage data: Companies can collect data on how users interact with their mobile app, including app usage, preferences, and in-app purchases.

The Importance of Consent Management in Building Consumer Trust

- In addition to the changing landscape of marketing and technology, getting consent management right on your platforms is vital. As a result, companies must prioritize consent management to build consumer trust and maintain compliance with data privacy laws.

- Consent management involves more than implementing a cookie wall for your website and cookies, and may also include opt-ins for newsletter subscriptions. To ensure proper consent management, it is necessary to provide a suitable solution that spans across all of your platforms.

Improve Collection of First-party Data:

Here are some ways to improve the collection of first-party data:

- **Offer incentives:** Encourage users to provide their data by offering something in return, such as exclusive content or discounts.
-
- **Be transparent:** Clearly communicate what data you are collecting and how it will be used. Provide a privacy policy that outlines your data collection practices.

- **Use data capture tools:** Implement data capture tools such as pop-up forms, surveys, and quizzes to collect more information from users.

- **Personalize content:** Use first-party data to personalize the user experience by showing relevant content and product recommendations.

- **Compliance:** Consent management is a critical component of compliance with data privacy laws, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). By complying with these regulations, companies can demonstrate their commitment to data privacy and build trust with users.

- **Provide value:** Provide value to users in exchange for their data. For example, a news site may require users to create an account to access premium content.

2. Contextual targeting:

- Contextual targeting is a digital advertising strategy that involves serving ads to users based on the content they are currently viewing on a website or app. This approach relies on analyzing the context of the content, such as the topic or keywords, rather than relying on individual user data like cookies or demographic information.
  - **How do we use it?**
    - To use contextual targeting, advertisers use machine learning algorithms and natural language processing to analyze the content of a webpage or app and identify relevant keywords and topics. They can then serve ads that are relevant to the content and the user's interests.
  - **Example:**
    - if a user is reading an article about travel, contextual targeting could serve ads for hotels, flights, or travel-related products. If a user is reading a recipe, contextual targeting could serve ads for kitchen appliances or food delivery services.
- **Discover Your Visitors:**
  - It's not feasible to collect email addresses or logged data about all website visitors. Knowing the interests of visitors and potential customers is essential to contextual targeting. Once interests are categorized, inclusion and exclusion lists can be created for better targeting. Regularly updating these lists is crucial to attract new visitors.

3. Behavioral targeting:

- In behavioural targeting, digital marketers collect the user’s browsing behaviour and activity details from various sources and use this information to design targeting ads relevant to the users. Behavioural targeting and advertising use cookies and pixels to collect these user details.

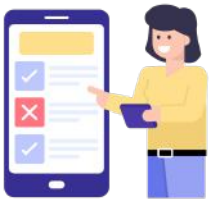
  - **Example:**
    - In behavioural marketing, marketers assume the user is a coffee lover based on their previous web activity, such as the websites they visited and searched.

Best Practices:

Understanding user interests is crucial for precise contextual targeting. Here are some ways to do that:

Analyze website behavior

Analyze the user's behavior on your website, such as the pages they visit, the products they browse, and the actions they take. This data can help you understand their interests and preferences.



Surveys

Conduct surveys to understand what users are looking for and what their interests are. You can also ask for feedback on your products or services to improve them.

Keyword Research

Conduct keyword research to understand what users are searching for related to your brand or industry. This can help you identify topics and interests to target.

User Login & Subscriptions

Logins and subscriptions provide valuable user data, allowing publishers to create personalized content, build relationships, and understand their audience.

Audience Segmentation

Based on the data collected, advertisers can group users into different segments based on their interests and behavior.

Monitoring Social Media

Monitor social media platforms to see what users are saying about your brand or industry. This can give you insights into their interests and what they're looking for.

DATABEAT

4. User IDs and Identity:

- **What is Universal/Unified Id?**
  - Universal IDs or Unified/Shared IDs are among the potential solutions for the emerging privacy-focused digital advertising ecosystem. These standardized cookie-based identifiers can be synced across various platforms, including desktops, mobile devices, and tablets, and function similarly to first-party cookies while behaving like third-party cookies.

- **Top ID solutions in the market:**
  - The Trade Desk, in partnership with Index Exchange, was among the first to propose a Unified ID Solution, while other providers, including the Advertising ID Consortium, LiveRamp, and ID5, Verizon media connectID, lotame panorama ID, NetID, Parrable ID, Pubcommon ID, Pubprovided, Quantcast also offer Universal User IDs solutions.

- **Here are few reference links to the top ID solutions:**
  - ID5
  - LiveRamp
  - Lotame Panorama

- **Benefits of connecting User IDs:**

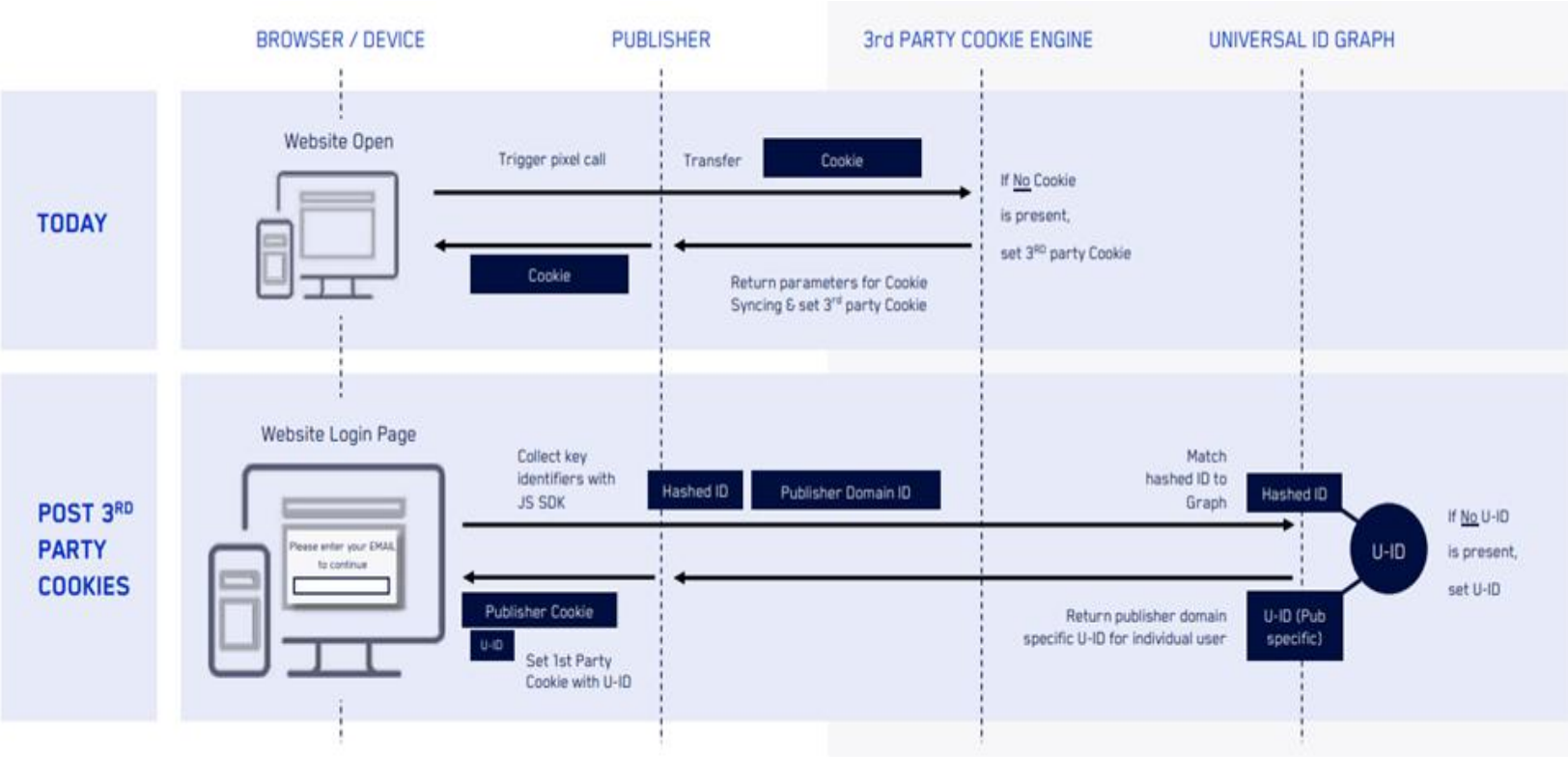
How Universal ID Implementation Differs from 3rd Party Cookies:

- Firstly, Universal ID is created and managed by a neutral party, typically a consortium of companies, rather than a single ad network or company. This allows for more transparency and accountability in how the ID is used and shared.

- Secondly, Universal ID is not tied to a specific domain or website like a third-party cookie. Instead, it is a persistent identifier that can be used across different domains and devices, enabling better cross-device tracking and targeting.

- Thirdly, Universal ID is based on hashed email addresses or other deterministic identifiers, rather than relying on less reliable methods like browser fingerprinting or probabilistic matching. This allows for more accurate and privacy-friendly targeting.

- Finally, Universal ID is typically implemented using a server-to-server integration rather than relying on client-side JavaScript like third-party cookies. This provides more control over data collection and reduces the risk of data leakage or unauthorized access



DATABEAT

Results of ID5:

- The prebid analytics results clearly demonstrated the ID5 ID's worth to publishers. SSPs that passed the encrypted ID5 ID to their DSP partners received more and higher CPM bid responses than those that did not.

AVERAGE BID CPM ACROSS ALL BROWSERS

AVERAGE BID CPM IN COOKIELESS ENVIRONMENTS

11%

Increased Bid CPM Overall

CPEx's average Bid CPM for ad opportunities where an ID5 ID was present was **11% higher** than when there was no ID5 ID present.

39%

Increased Bid CPM in Cookieless Environments

The average Bid CPM for ad opportunities in cookieless environments, such as Firefox, Safari and Edge, where an ID5 ID was present was **39% higher** than when it was absent.

Results of LiveRamp:

- Below results are from one of our publisher

Dimensions	Without ID	With ID
CPM	$0.82	$0.98
Fill Rate	3%	8%
Match Rate	37%	62%

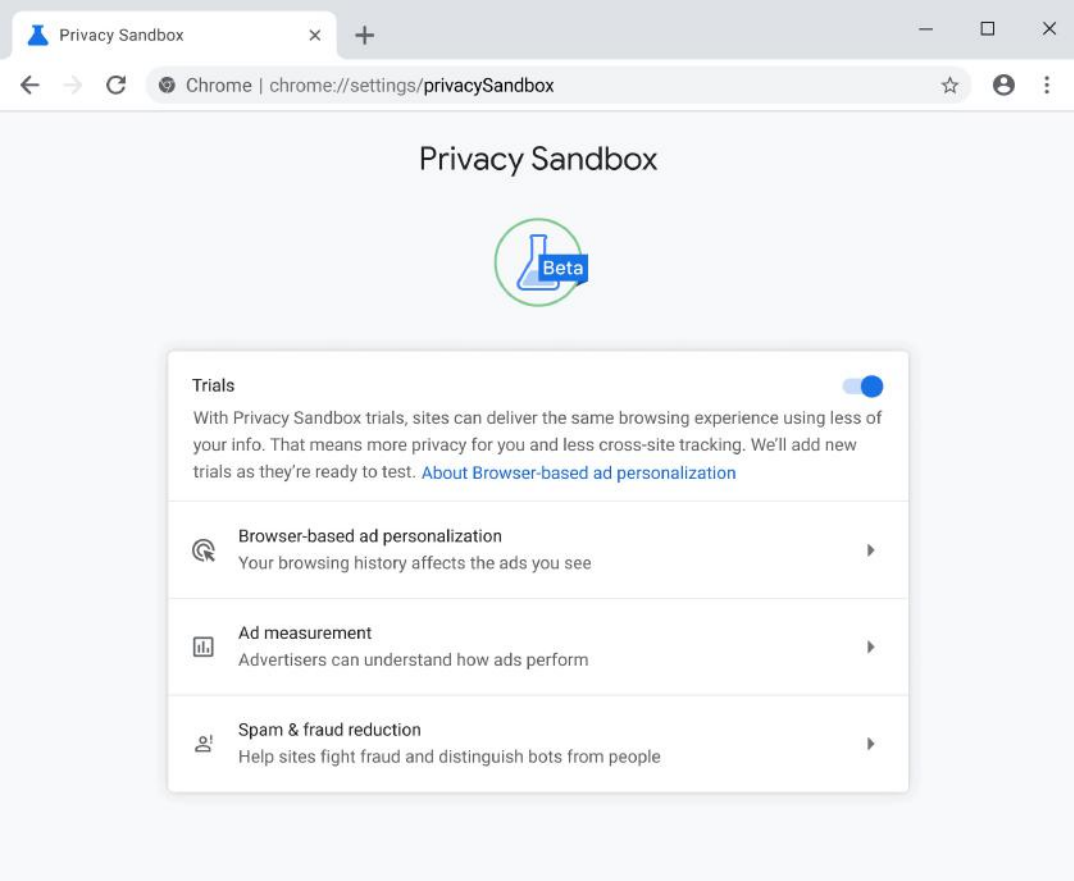
5. Google's Solutions: "Privacy Sandbox"

We believe that the Privacy Sandbox will provide the best privacy protections for everyone. By ensuring that the ecosystem can support their businesses without tracking individuals across the web, we can all ensure that free access to content continues.

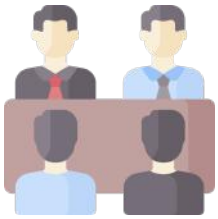
It's important to note that the Privacy Sandbox was created as part of Google's roadmap for the future of the open web (and to comply with anti-trust laws). The two primary goals are to:

1. Improve user privacy
2. Provide businesses with insights and tools for a successful online strategy.

For the Privacy Sandbox trial users, they will see a prompt like this:



How Would Google Privacy Sandbox Work?



FLoC

This will be a key that will be used to club the users together based on their interests. The data from the browsing history will be used to determine the interest. Creating flocks will help in concealing the personal identities of the users.

Trust Token API

Publishers can use this API to distinguish between human and bot users, allotting cryptographic tokens to trusted and non-trusted users without tracking them. By requesting users to fill out a form, fraud detection can occur without compromising user privacy.

Aggregated Reporting

As the name suggests, this API will be used for reporting needs. Performance-related information like impressions, views, reach, etc would be collapsed into a single report without cross-site tracking of the user.

Conversion Measurement

This API will help advertisers in finding out whether a user was converted by clicking on the ad or buying the advertised product.

Privacy Budget

This feature will limit the sites in collecting user data and types of signals. A budget will be allotted to the site for retrieving data from the APIs. In this way, only the most necessary user data will be passed to the website.

First-Party Sets

It would enable publishers to declare multiple domains owned by them as the same first-party.

Here are some of the top browser APIs that can potentially replace cookies:

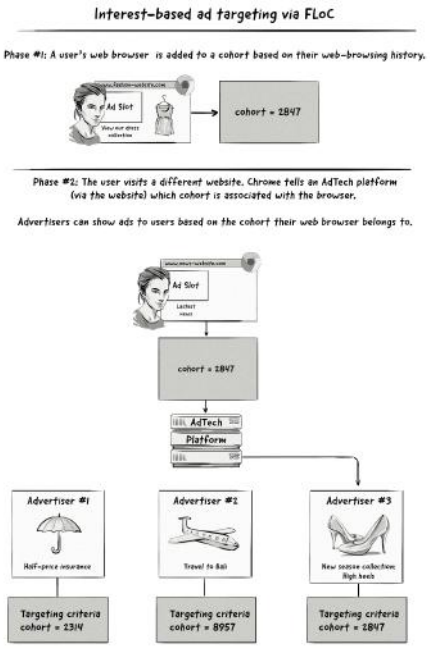
1. **FLoC:**

Google has been working on the Privacy Budget concept, which allows websites to collect limited user data without requiring approval for each individual user. In a cookieless environment, this strategy is intended to assist bridge the gap between the need for personalized advertising and user privacy concerns. Privacy Budget tries to balance the benefits of data collection with the requirement for privacy protection by keeping track of how much data is collected and suitably limiting it.

What are the Benefits of FLoCs?
Advertisers are more interested in serving Interest-based ads to the users, as they believe it will be more relevant to the users. To serve interest-based ads, advertisers are relying on third-party cookies which are causing privacy issues to the users and that's where FLoCs come in.

FLoCs would eliminate the need for advertisers to drop third-party cookies on the user's browser to track & serve interest-based ads around the web.

Does FLoCs Work Only on Chrome?
Yes, as Federated Learning of Cohorts (FLoCs) is created by Google for its browser, it works only on Chrome. It might be extended to other browsers in the future.



2. Privacy Budget:

Google has been working on the Privacy Budget concept, which allows websites to collect limited user data without requiring approval for each individual user. In a cookieless environment, this strategy is intended to assist bridge the gap between the need for personalized advertising and user privacy concerns. Privacy Budget tries to balance the benefits of data collection with the requirement for privacy protection by keeping track of how much data is collected and suitably limiting it.

3. Trust Tokens:

A way to verify that a user is human without relying on cookies or other tracking methods.

Here's how Trust Tokens work in more detail:

- A user visits a website and requests access to a protected resource, such as a login page or an online form.
- The website generates a Trust Token and sends it to the user's browser.
- The user's browser signs the Trust Token using a secret key that is unique to that browser.
- The signed Trust Token is sent back to the website, which can verify that the token is valid by using a public key that is associated with the user's browser.
- If the Trust Token is valid, the website can grant access to the protected resource

4. IndexedDB:

This is another browser API that allows websites to store larger amounts of data on the user's device, up to a certain limit. This can be used as an alternative to cookies for storing user preferences and behavior data.

5. Cache API:

This browser API allows websites to store static resources, such as images or scripts, on the user's device for faster loading times. This can be used to track user behavior by identifying which resources are accessed and when.

How can DataBeat help?

In a cookieless future, where user tracking and targeting becomes more difficult, Databeat can play an important role in helping advertisers and publishers adapt to new identity solutions and maximize their revenue and return on investment.

Analyze Data

Optimize targeting strategies

Identify Trends

A/B Testing

Implementing Identity Solutions:

Data integration
Data mapping
Data quality
Scalability

Monitor and Optimize Programmatic Advertising

DATABEAT