

Marketers: Are you prepared for life after third-party cookies?

Understanding the implications of the third-party cookies phase-out.



Contents



- 03 Introduction
- 04 What are third-party cookies?
- 05 The progression of the web
- 06 What is the Privacy Sandbox?
- 07 Privacy Sandbox: technology proposals and development
- 08 Problems the Privacy Sandbox will solve
- 10 Concerns over Google's Privacy Sandbox
- 11 What will this mean for advertisers?
- 12 The importance of owning first-party data
- 13 Increased focus on account-based marketing (ABM)
- 15 Why you shouldn't deploy fingerprinting
- 16 Reverse IP tracking technology
- 17 Web Insights: helping you prepare for the third-party cookies phase-out




Introduction



With rapidly evolving regulatory restrictions, Google announced in early 2020 that it would stop using third-party cookies in Chrome. In doing so they joined a growing list of browsers including Safari and Firefox who have already phased them out.

While Google had planned to phase third-party cookies out by 2022, that date has now been pushed back to 2023, with developers citing that more time is needed to ensure this is done correctly.



Our guide will explain everything you need to know about third-party cookies being phased out, what new technologies are being proposed as their replacement, and what strategies and tactics you can deploy now in preparation for these changes to safeguard your business.



What are third-party cookies?



You might already know what a third-party cookie is, but just in case here's a refresher.

Third-party cookies are those that do not originate from the website operator, but a third party such as an advertiser. These cookies record a user's behavior and path on the internet, creating a user profile. Using this profile, targeted and personal adverts are displayed according to the user's interests and web-based behavior.

How are third-party cookies used?

Digital marketing uses third-party cookies in particular for targeting, tracking, and re-tracking. Because of this, third-party cookies are considered one of the most effective online marketing tools.



The progression of the web



To understand the implications of the changes to third-party cookies, it helps to understand the background for why the changes are being implemented.

Cookies have moved beyond their original purpose, many feel they are invasive

There has been a substantial amount of public discourse over the information collected by third parties and the privacy implications of this. There are many claims that these tools have moved beyond their original purpose and have become invasive and a threat to data protection.

In recognition of how invasive this tracking has become, the EU's data protection laws classed cookies as "online identifiers", subject to regulations requiring websites to gain consent before issuing cookies to a browser.

Google is developing alternatives to third-party cookies

However, users are still demanding greater privacy including transparency, choice, and control over how their data is used and it's clear the web ecosystem needs to evolve to meet these increasing demands.

Holding **64% of the market share for all web users**, Google is carefully planning the alternatives to third-party cookies and as a result of this, has introduced the **Privacy Sandbox**. The initiative aims to protect people's privacy online as well as keep the web open and accessible to everyone, businesses included.

"If digital advertising doesn't evolve to address the growing concerns people have about their privacy and how their personal identity is being used, we risk the future of the free and open web"

- David Temkin, Director of Product Management, Ads Privacy and Trust at Google



What is the Privacy Sandbox?



The Privacy Sandbox is Google's collaborative, open-source effort to develop new technologies, prioritizing user privacy protection without negatively impacting critical web functionality.

The Privacy Sandbox is continually being worked on, but these new technologies are being designed to:

- Prevent tracking as individuals browse the web.
- Enable publishers to build sustainable sites that respect privacy.
- Preserve the vitality of the open web.

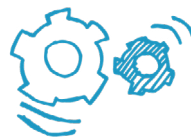


Google's new technologies will be scaled across the web in mid-2023

According to their **updated timeline**, Google plans to deploy these key technologies by 2022 for developers to start incorporating them. Once these have been adopted they will launch in Chrome and be scaled across the web over a three-month period starting mid-2023 and ending in late 2023.

In developers' language, a 'sandbox' is an isolated environment and a safe place for testing that can't affect anything outside of it; Google has created a developer sandbox for Google Chrome, where companies or individuals can 'play' with the Google Chrome browser data.

Privacy Sandbox: technology proposals and development



Out of the 30 privacy-preserving technology proposals submitted to Google, four have been chosen so far and are currently in development.

Each of these new proposals will go through a meticulous multi-phase development process which includes:

Public development process

- Discussion - technologies and prototypes are discussed in forums
- Testing - multiple trials which encourage transparency and feedback throughout
- Ready for adoption - with the development stage complete, successful technologies will be launched and scaled

Two-stage phase-out

- Stage 1 (starting late-2022) - publishers and advertisers will be given approximately nine months to migrate their services
- Stage 2 (starting mid-2023) - support for third-party cookies phased out over three months



Problems the Privacy Sandbox will solve



The Privacy Sandbox has four critical areas of focus and aims to solve the problems that will arise from removing third-party cookies:

1. Ad targeting

How will digital marketers reach users interested in their products? Can they reach their ideal customer profile (ICP)?

Proposals: **FLoC** & **TURTLEDOVE**

FLoC uses machine learning to reach new audiences by grouping them with a cohort of similar people (keeping them anonymous). TURTLEDOVE focuses on retargeting; adverts are served on interests and data is held by the browser, not advertisers.

2. Ad delivery

After reaching the correct customer, how will the right ads be served to them?

Proposal: **Fenced Frame** & **The Trust Token API**

These will be similar to iframes, but separate from everything else on the page. This will allow adverts to be embedded and displayed, whilst keeping users' information private from the advertiser. For example, example.org cannot access any information from example.com as there is a fence around it.

Previously, third-party cookies were used to track behavior and associated stable identifiers to prove authenticity across sites. This will be replaced by a privacy pass token that segments users into trusted and untrusted sets that are non-personalized. This will prevent fraudulent traffic or spam actors.





3. Ad performance and conversion measurement

How will advertisers get accurate reporting of their paid campaigns?



Proposal: **Aggregated Reporting API and the Conversion Measurement API.**

The browsers will store information based on activity. Then the browser will send back the aggregated information to the advertiser.

4. User privacy

How will users maintain their privacy?

Proposal: **The SameSite Attribute & The Privacy Budget**

The SameSite Attribute ensures first and third-party cookies are marked for easy identification. When they are marked, browsers can easily block them.

The Privacy Budget will mean every website will have a budget (which is the amount of information) that it can use to request from the browser. A website can't go beyond that allocated privacy budget, preventing **fingerprinting**.



Concerns over Google's Privacy Sandbox



There have been some concerns over the phase-out of third-party cookies; particularly around how Google could have an advantage over their competitors, and that the technologies being developed as alternatives will be even more invasive and a bigger threat to users' privacy.

The end of third-party cookies doesn't mean the end of consent



Just because third-party cookies are ending, this does not mean persistent and pervasive tracking is going to stop. In fact, there are concerns that Google will still have access to individual-level user web data, whilst denying that opportunity to competitors and service providers — giving them a clear advantage. This is currently what the authorities are focusing on, instead of focusing on what is important, which is users' privacy.

The Privacy Sandbox could strengthen tracking

The Privacy Sandbox technologies being developed could also strengthen tracking, especially as they aim to continuously re-identify users, which will allow for tracking precision.

As a result of this, an industry regulator is being advocated for. In addition to this, consent is being advocated for, as this will truly allow for any changes made to the ecosystem of the web to uphold user privacy interests first and foremost.



Consent is the platform for compliant tracking today and in the future.

What will this mean for advertisers?



In an ideal world, this will not impact advertisers.

During tests, one of the proposals, FLoC, is reported to have **at least**

95%

of the conversions per dollar spent when compared to cookie-based advertising.



However, third-party cookies are the cornerstone of online advertising campaigns, and phasing out third-party cookies will be a drastic transformation, creating an entirely new landscape for digital marketers.

What are the short-term solutions?

Above and beyond Google's new technologies and proposals, currently, a few alternatives are emerging as replacements;

First-party data collection

Account-based marketing

Fingerprinting

Reverse IP Tracking



The importance of owning first-party data



What is first-party data?

Google defines first-party data as information collected from customers, site visitors, and app users during their interactions with your enterprises' products and services. To be considered first-party data, information must be collected from your own sites, apps, physical stores, or in other situations when people have directly interacted with the products and services your business offers.

First-party data is more transparent

With first-party data, consumers give their data directly to organizations instead of being unknowingly tracked by third parties. This can be viewed as more transparent as it creates a clearer 'value exchange' with customers and prospects knowingly giving their data in exchange for content or other incentives and services.

First-party data will become even more important

As third-party cookies are phased out, having a strong first-party data collection strategy will be crucial for digital campaigns moving forward, as they will ensure that your business has compliant, actionable data on your audience's activity.

Simply put, if your enterprise relies on borrowing data for campaigns from Google, the focus now needs to shift to owning it.

However, even though first-party data is more compliant with privacy regulations and is easier to navigate with regards to user consent, without the right tools quality first-party data can be even harder to obtain than third-party cookie data.

85% of marketers state that improving their first-party data usage is a high priority.

Increased focus on account-based marketing (ABM)

What is ABM?

Account-based marketing is typically employed in enterprise-level sales organizations. It's a personalized and strategic approach to B2B marketing that focuses on account awareness; targeting individuals, departments, and particular companies.



How does ABM work?

The aim is to identify existing high-value accounts that can then be used to identify new prospects that fit the same profile and are more likely to convert. Once these accounts have been secured, the idea is to offer them an increasing amount of services, improving the customer lifetime value for your enterprise by building and fostering relationships. After all, retention is key in delivering excellent ROI in B2B, and it is well known that it is cheaper to retain customers than acquire new ones.

With the changes, more targeted approaches will be used

As third-party cookies are phased out, this will result in less scope for broad-brush online marketing. Refined and targeted approaches, such as ABM, that focus on an ideal customer profile (ICPs) will become more prominent as a result of this.



First-party data can invigorate ABM activity

With first-party data collected through ABM, your enterprise can gain data-informed metrics on a prospect or existing accounts behavior, you can better **personalize your communications** and offer a tailored solution depending on their needs.

Companies with more data are better prepared for ABM

Naturally, larger organizations with a deeper pool of first-party data will have more to work with. However, smaller organizations with less access to first-party data — or those who have not invested in collecting audience data from subscriptions, newsletters, etc. — will not be as well equipped for the new advertising landscape.

ABM is also a long-term strategy that requires a lot of time, effort, and resources which can be a challenge especially when companies need quick wins and need to ensure a steady flow of revenue at all times.



Why you shouldn't deploy fingerprinting



What is fingerprinting?

Fingerprinting is another tactic used to track a user's behavior and information in digital marketing. Device fingerprinting, also known as browser, canvas, and machine fingerprinting, identifies devices based upon their unique configuration. This differs from third-party cookies which are stored on a user's browser, whereas device fingerprints are stored server-side.



How is it used?

Before its use in digital marketing, fingerprinting was used to prevent software privacy and credit card fraud as it acts as a user identifier. Now, it is used to identify a user's activity across devices. While third-party cookies can be blocked or deleted, fingerprints are difficult to remove once they have been collected.

Leading browsers are working to block fingerprinting

While this alternative has been appealing for digital marketers as an alternative to cookies, the leading browsers, including Google Chrome, have been working hard to forestall fingerprinting to further protect consumer's privacy.

In a blog post, **Google** stated that *"many publishers rely on cookie-based advertising to support their content efforts, and we have seen that cookie blocking was already spawning privacy-invasive workarounds (such as fingerprinting) that were even worse for user privacy"*.

In conclusion, this is not a viable alternative and should not be deployed as a tactic to counteract third-party cookies.



Reverse IP tracking technology



What is reverse IP tracking?

Reverse IP tracking technology, or **website visitor identification software**, goes a step further than regular IP tracking by querying the domain system name (DNS) associated with an IP — revealing who owns it.

How does it work?

In essence, this enables organizations to undertake reverse IP lookups and access the top-level domain data produced by an IP. Users receive the name of the company hosting that IP alongside additional details of those registered to it, too.

Reverse IP tracking provides rich data on your website visitor's activity.

Organizations that leverage this technology obtain in-depth first-party data on their website visitor's activity. With this, they can fuel every aspect of their marketing activity by having data-informed insights. This is a highly viable alternative as it does not require borrowed data from third-party cookies. Instead, organizations own the data on the audience in a way that is compatible with the changes.

However, a challenge for many organizations is finding website visitor identification software that provides high-level engagement insights for their high traffic websites while meeting their company needs.



Web Insights: helping you prepare for the third-party cookies phase-out

Planning ahead for these changes is vital

Whilst Google is doing everything they can to ensure this transition is smooth and that the ecosystem of the web is maintained moving forward, without impacting paying publishers, it's essential to plan and be prepared for what could potentially be a negative impact on business.

Marketers need to ensure they still have account-level data after the changes

As the B2B marketing landscape shifts to accommodate users' privacy, marketers need to ensure they still have the account-level data to power strategies and digital campaigns. This can be done with the viable alternatives mentioned; first-party cookies, deploying ABM strategies, and using reverse IP tracking such as **Web Insights**.

Reverse IP tracking is the most viable solution to fuel your campaigns

Reverse IP tracking will also aid first-party data collection and ABM campaigns, making it the most prominent of solutions and a clear favorite in response to the changes to third-party cookies.

Web Insights is an industry leader in reverse IP Tracking, with over 1.4 billion addresses and an additional 55 million addresses added to that database every year. But beyond having the largest database, users' privacy has always been at the forefront of our business.






Web Insights is an industry-leading solution

Our website visitor automation is an excellent tool in preparation for the changes to third-party cookies, and for the marketing landscape that will follow once these changes have been implemented — all whilst putting users' privacy first.

We are fully compliant with all the global laws, including GDPR, ensuring all personal information is protected and privacy is maintained.

Our website visitor automation is also an industry-leading solution. It allows for two-way integration and can be plugged straight into your CRM or marketing automation software. The automation of this process allows data collection for high website traffic volumes to be effortlessly streamlined.





Close **more business** than ever before, and
accelerate business success with **Web Insights**.
Real-time engagement; real-time success.

[Book a demonstration](#)

UK: 02039 932 497 | **US:** 508 206 8428