

EX1036

[Home](#) > [Blog](#) > [Ad-tech](#) > [What are Browser Cookies? The History of Cookies in Digital Advertising](#)

What are Browser Cookies? The History of Cookies in Digital Advertising

Magdalena Bober • 27 Jul, 2023



The Internet has come a long way since its humble beginnings in the 1960s. While the original purpose of the World Wide Web was to exchange data between computers, it soon grew in size, space, and functionality. It became a source of information, a new way of shopping, a social space, and a medium of entertainment.

Before the Internet evolved to its present form it was a lot less practical. Each visit was a separate, completely anonymous event. But that didn't work so well for many sites, especially e-commerce ones. As *necessity is the mother of inventions*, it was necessary to give the web a memory.

And thus cookies were created. They allowed websites to keep track of who visits them and what they're looking at. It wasn't long before the advertising industry saw the immense potential of using cookies to personalize ads.

If you're curious about the peculiarities of cookies and how they transformed the advertising industry, read on and learn how a small text file can cause so much controversy.

What are cookies?

Cookies, often referred to as HTML cookies, HTTP cookies, Internet cookies, or browser cookies, are small text files used to identify individual users browsing the web. They are **indigenous to the visited websites and are stored on the user's computer via web browsers**. Essentially, cookies allow each site to recognize a user as the same person that has visited the site before.

In practice, when you visit a website it drops a cookie on your computer. That cookie keeps you logged in and keeps track of your activities (such as setting filters while browsing a store or storing items in your cart). When you visit next time, the site knows it's the same person again.

[Cookies can have different purposes as well](#). While we'll discuss the types of cookies in the next section, they all serve one of the following two purposes:

- **Managing a single browsing session** – these are the cookies briefly described above. They keep track of browsing activities within the same session, thus ensuring a smooth user experience and streamlined e-commerce transactions.
- **Managing multiple separate sessions** – these are the cookies that are able to identify an individual user over multiple separate sessions. They're used in cases such as keeping users logged in or saving browsing preferences and history.

What are different the types of cookies?

Apart from the most popular distinction into third-party and first-party cookies (to be discussed below), HTTP cookies can be divided by the period of activity.

Session cookies – also called transient cookies or temporary cookies, last only one same site session. A session cookie is not stored on the hard drive and is deleted as soon as the user is done browsing the site. This is the cookie that has a unique session identifier that allows it to recognize a single user as they move through the site.

Persistent cookies – also referred to as permanent cookies, last over multiple sessions. Among the most popular ones are tracking cookies and authentication cookies, however, their range of functionality also includes remembering any changes made to a website including language, theme, favorites, preferred shipping addresses, payment methods, etc.

Flash cookies – are no longer in use, however, they were not a type of HTTP cookie. They weren't stored in the browser but in the Adobe Flash browser application. Because of that, they had to be managed (cleared) separately.

Before the [end of Adobe Flash Player in late 2020](#), flash cookies were the most popular type of zombie cookies. **Zombie cookies** take the form of a small bit of code (rather than a text file) which is capable of recreating removed HTTP cookies. Flash cookies were also extremely difficult (or impossible) to delete which, in 2010, has [brought on a lawsuit](#) on companies who used them.

Third-party vs. First-party cookies

The biggest distinction in browser cookies is based on who the cookie belongs to. There are no other technical differences, meaning, both cookies are the same in characteristics but different in origin and usage.

A **first-party cookie** belongs to the owner of the website. It's created by the host domain and its main purpose is to manage the single browsing session. It remembers what users are doing, what parts of the website they're visiting, and the changes they make to the site (e.g. adding items to the shopping cart). Apart from ensuring a good web browsing experience, first-party cookies collect analytical information that can only be accessed by the owner of the website.

A **third-party cookie** belongs to someone other than the website owner, e.g. an ad tech platform. The main purpose of a third-party cookie is to track user activity across the web. Sometimes, these cookies are used to provide third-party services (such as a live chat), however, most of the time, they're used for online advertising activities.

How are first-party cookies used in advertising?

First-party cookies are generally not used in advertising. They belong to the website owner and they can only be used by the said owner. There are, however, [some exceptions](#). First-party data can be stored in data management systems. From there, it is possible to share it with third-party vendors. First-party data can also be shared as a form of partnership between websites.

How are third-party cookies used in advertising?

Third-party cookies are an integral part of the web pages that millions of users visit on a daily basis. The browser stores them on a user's computer, essentially allowing the third parties to gather an extensive profile of each unique user on their web server. And if a certain ad company knows the location, reading habits, interests, and recent purchases of a single individual, they can target and retarget ads between various sites and companies to serve ads of products that individual is actually interested in.



The **Placement Categories** update is now **LIVE!** Enjoy the new supply categorization and granular insights into the platform. [Explore](#)



Also, web pages used to have no limits on storing cookies. Before regulations introduced by Apple, Mozilla, and finally Google, each user could have been tracked by multiple 3rd-party cookies at the same time. That way, a user's browsing history, preferences, areas of interest over multiple visits, user's shopping cart, and various other data was known to other websites and used for the purpose of ad targeting.

Are cookies good or bad?

The answer to this question is not straightforward. Cookies have a purpose – to remember what a user is doing and where just so they can facilitate a smooth web browsing experience. Thanks to cookies, we stay logged in, we have a list of favorites and we receive ads of products we looked at. Cookies can provide users with ads of products they wanted to buy anyway but with a special discount. They can be useful but at the cost of privacy.

It will be clear from the following section why third-party cookies are slowly eliminated. However, before we judge cookies as either good or bad, it is important to learn what they're capable of and where the privacy concerns are coming from.

What cookies can:	...and cannot do:
Collect user information Track user behavior Remember the products and ads that were clicked on Know location and device Be hijacked in cyberattacks	Can't obtain personal information from your computer Don't contain viruses Have no access to your passwords Can't make changes in settings

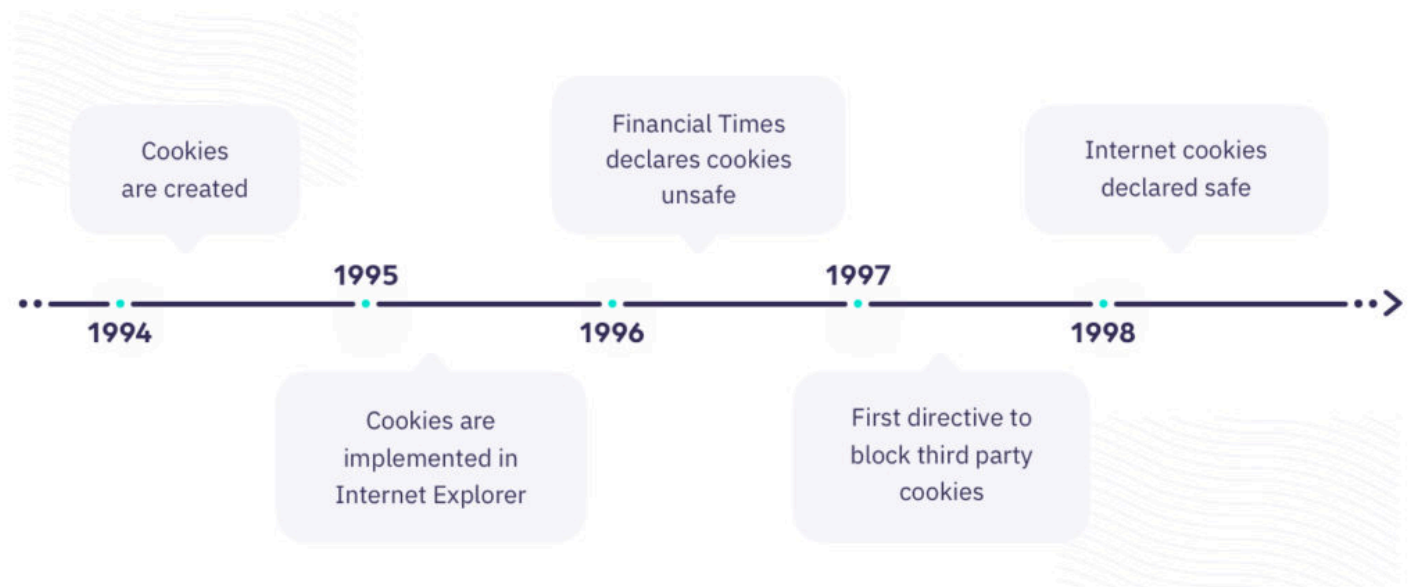
The early history of cookies

To understand the current attitudes towards cookies we need to take a look at their history. Cookies were created in 1994 by Lou Montulli, a web browser programmer at Netscape Communications. The idea behind cookies was simple – **they would allow people shopping at an e-commerce site to store their items in a virtual shopping cart.** As reported by [The New York Times](#), this was the first instance in the history of the Internet where a website's data could be reliably stored on a user's computer.

In 1995, Montulli applied for the [patent for the cookie technology](#), and just the same year it was implemented in version 2 of Internet Explorer. Although cookies have already become an integral part of the web experience, they were working entirely behind the scenes.

This is where the first concerns appeared as well. While the public enjoyed the comfort that came with individual tracking, the more tech-savvy user raised their concerns. That led to the publication by the [Financial Times](#) in February 1996. It wasn't what the cookies were that alarmed people, it was what they might be used for.

And thus the issue of consumer online privacy was born. Let's remember that at that point in time, cookies were not used for advertising purposes. It didn't mean, however, that their potential wasn't noticed and considered in a much broader light that far exceeded their initial purpose.



The first directive to block third-party cookies

The realization that cookies could be shared with and exchanged between their origin websites and across a whole network of sites made cookies, and to be exact, third-party cookies a hot topic. **Within a year, the existing advertising companies have already begun exploiting third-party cookies to track users and follow them around with ad campaigns.**

This is also the reason why the Internet Engineering Task Force's recommendation ([RFC 2109](#)) to block third-party cookies was not followed. Both the then-popular Netscape Navigator browser and the newcomer Internet Explorer ignored the plea. The browsers were set to automatically accept third-party cookies and, at the time, there was no way of enforcing a different state of action.

To curb the arising negativity and dispel any rumors, the Computer Incident Advisory Capability (CIAC) [released a statement](#) explaining exactly what cookies are and what they are not. Here is the beginning of the statement:

The popular rumors about web cookies describe them as programs that can scan your hard drive and gather information about you including: passwords, credit card numbers, and a list of the software on your computer. None of this is close to the truth. A cookie is a short piece of data, not code, which is sent from a web server to a web browser when that browser visits the server's site. The cookie is stored on the user's machine, but it is not an executable program and cannot do anything to your machine.

The start of a war on third-party cookies

Coming into the 21st century, the ad tech industry was becoming adept at utilizing third-party cookies. In 1999, DoubleClick (one of the biggest internet advertising companies, now part of Google) had planned to [merge with a company specializing in collecting user's personal data](#) for the purpose of online advertising. The negative public reaction was so severe that the plan had to be abandoned.

[In 2000, another RFC directive was released.](#) This highly technical document specified **how and when each kind of cookie is supposed to be used**. This was supposed to cater to the needs of the browsers that didn't comply with the RFC 2109 directive. Unfortunately, that didn't happen. The new types of cookies were hardly ever used and quickly sunk into oblivion.

Rapid gathering of third-party data

In the meantime, the usage of cookies runs rampant. According to [the investigation done by The Wall Street Journal in 2010](#), user data was being regularly exchanged for website access. The 50 sites checked by TWSJ have installed over 3,000 tracking files on the computer used in the study.

As expected, it was the ad tech giants that were tracking users most scrupulously. The concept of user privacy was slowly disappearing. Some sites didn't allow for blocking third-party cookies and although tracking was disclosed in the privacy policies, the extent of it was further than people could imagine. The [2002 ePrivacy directive](#), requiring websites to inform users about what data is being tracked and allowing them to opt-out was not entirely successful.

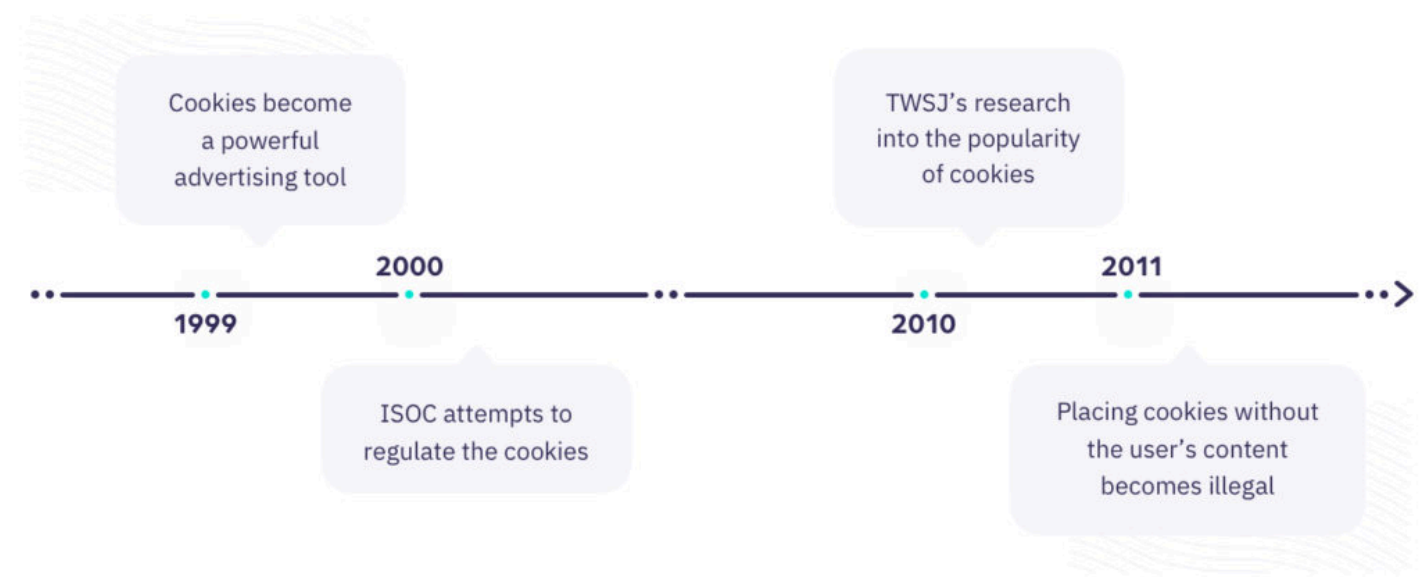
Third parties would not only gather data on users' behavior, and location, but also on their age, gender, income, marital status, health concerns, purchases, and interests. Some would go as far as recording keystrokes thus completely violating consumer privacy in the race for the most accurate data collection.

The cookie law

The unrestrained user tracking finally led to firm actions from the Federal Trade Commission and the European Union. In 2011, the Cookie Law came into play. Otherwise known as the [Directive 2009/136/EC](#), it established that it's illegal to place third-party cookies on a user's device without their consent. Companies were no longer allowed to collect data without informing users and receiving their permissions.

Of course, the directive didn't include first-party cookies or any other tracking technologies used to provide a smooth user experience. It was simply the breakthrough moment when **all of**

the pop-ups started appearing asking users for permission to collect third-party data. An ad network could still target ads but only to those who explicitly consented.



Why are third-party browser cookies disappearing?

The web community has always been skeptical about web servers gathering information about user browsing habits. After all, cookies store not only information necessary for the functioning of websites, but also information about their interests and interactions. That might include sensitive data and personally identifiable information.

Cookies created without user consent could follow individuals around the web. Despite [GDPR laws and directives](#), consent pop-ups were still designed to trick users into accepting browser cookies. And while it was possible to delete cookies, some (like Zombie cookies) would stay on the visitor's computer without their permission, thus propelling shady advertising practices.

That prompted a new privacy-oriented trend. Started by Apple in 2015, browser cookies were given less and less power in favor of user control. Despite the ad tech industry's reliance on permanent cookies, the biggest web browsers on the market started taking these security concerns seriously. After Apple has enabled ad blocking in Safari, other browsers followed with increasingly stricter cookie policies.

A timeline of browser cookie phase-outs

2015 – [Apple allows third-party ad blockers on Safari](#). Users who didn't want to see any more ads could simply install an ad blocker from the app store. A browser cookie that would normally

be 'hidden' in an ad, would no longer be able to land on the user's computer.

2017 – [Apple's Intelligent Tracking Prevention 2.0](#) disables browser cookies coming from third parties. Users would still be shown ads, however, as Safari wouldn't accept cookies from the publishers of the ad, the data stored in a cookie was no longer available. Hence – no accurate tracking and revenue attribution.

2019 – [Mozilla introduces options for handling cookies](#) and the option to disable cookies coming from third parties. This decision affected mainly smaller publishers but it paved the way for other browsers to further disable cookies used for tracking.

2019 – [Apple's Intelligent Tracking Prevention 2.2](#) limits the tracking functionality of first-party cookies. So first-party data became only accessible for 24 hours which didn't restrict website functionality but made it difficult to analyze data coming from complicated funnels that used first-party cookies.

2019 – [Google announces the Privacy Sandbox](#). As the browser that relies most heavily on advertising revenue, Google Chrome was most reluctant to introduce any changes. That's why the Privacy Sandbox project was meant to focus on finding alternatives to persistent cookies rather than removing them completely.

2020 – [Safari introduces automatic third-party cookie blocking](#).

2020/2021 – [Google announces plans to gradually phase out third-party cookies by early 2023](#). Initially, the plan was to be realized by 2022, however, Google keeps postponing further steps due to the ongoing development of alternative tracking solutions and the rejection of FLoC by all major browsers.

2021 – [Mozilla introduces total cookie protection](#) completely limiting tracking its users across multiple sites.

2022 – Google abandons FLoC in favor of a new, less controversial solution – [Topics API](#).

By mid-2021 cookies have slowly become obsolete. While first-party cookies are here to stay, third-party data will no longer be gathered and shared between the ad tech giants and the rest of the advertising industry. If every time a user starts an app they are asked for permission to be tracked, they will only agree only 25% of the time, [as shown by the most recent Apple update](#).

These developments have brought cookies back to their primary form. They're once again used to make the browsing experience easier and more convenient without infringing on user privacy.

What's the future of advertising?

There is no place for third-party cookies in the future of advertising. After third-party cookie-based ad formats peaked in the 2010s there's been a growing tendency towards more privacy-oriented solutions.

It was Apple that started the trend of giving consumers more control over being tracked around the web for the purpose of ad targeting. Consequently, the attitudes have changed and now all of the major browsers are either limiting or eliminating third-party tracking altogether. Thus, old targeting and retargeting methods are no longer working. There is, however, more space for alternative advertising solutions, be it first-party data, contextual targeting, or a yet-to-be-discovered technology.

Google, Facebook, and other tech giants who are most affected by the changes will continue to search for alternative methods of keeping their ad businesses alive. In the meantime, the last bits of third-party advertising is dying and brands are moving to cookieless ad formats.

Conclusion

As for the ad tech industry, it is hard at work trying to replace browser cookies with other methods of effective advertising. For the past couple of years, it's been clear that browser cookies coming from third parties (tracking cookies) are not welcome anymore.

Some of the largest companies in the world are now in the rush to future-proof their advertising. To answer the suddenly increasing demand, innovative and cookie-less ad formats are starting to emerge. These can not only bring customers to the desired website without cookies or any other third-party tags or trackers but also do it more effectively than traditional ad formats while maintaining brand safety and user privacy.

**Drive efficient sales to your brand
with Commerce Media solutions**

No cookies involved!

[Learn more](#)**Magdalena Bober****ZEROPARK****team internet.****Tags:**

Advertising strategies

Brand Safety



Follow The Signal

Subscribe to [The Signal newsletter](#) by Zeropark & **stay on top of the latest trends** with industry updates delivered straight to your inbox!

First name*



Business email*

☐

I agree to receive commercial information regarding Zeropark via email.*

[You may withdraw your consent at any time show more](#)

Commerce Media Tech Sp. z o.o., Krakow, Poland, is the controller of your personal data. It will be processed to send you The Signal newsletter and for our marketing purposes. Please see more information [here](#).

Subscribe



Solutions

Publishers

Brands and Agencies

Media Buyers

Resources

Blog

Demo

Documentation

About us

Media Planner

The Signal Newsletter

2024 Consumer Trends Ebook

Black Friday Report

2023 Consumer Trends Ebook

Events

Webinars

Careers

Legal

Advertiser T&C

[Publisher T&C](#)

[End-User Privacy Policy](#)

[Privacy Policy](#)

[Cookies Policy](#)

[DPA](#)

[Security](#)

© 2024 Zeropark by Commerce Media Tech