



End of third-party cookies

And how it will impact you

Local publishers are being forced to rethink their digital ad strategy as powerful targeting capabilities disappear.

Over the past decade, advertisers have shifted large amounts of ad dollars to digital platforms because they are able to target increasing volumes of customers with highly relevant ads, measure ad campaign success, and adjust marketing spend in real-time. This methodology is enabled by web browser coding called third-party cookies. They track users' browsing from site to site to build sophisticated user profiles based on interest. Advertisers can purchase these profiles for targeted marketing.

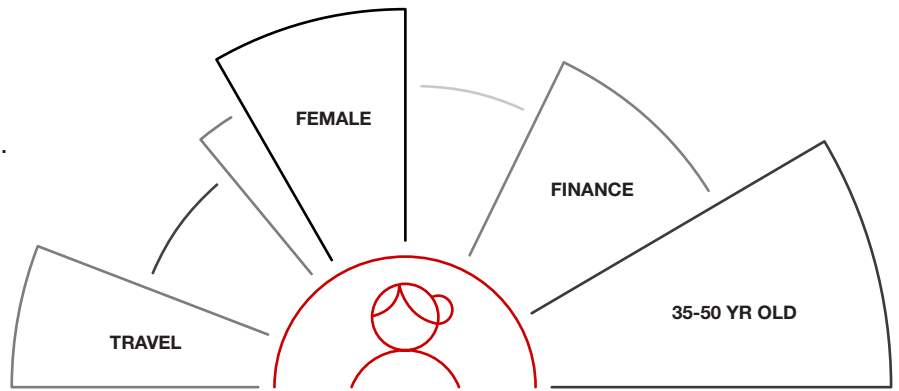
That's all about to change. Many consumers feel third-party cookies are a violation of privacy. They want to have greater control over how their personal information is stored and used. Regulators largely agree with them.

Google Chrome plans to end support for third-party cookies by 2022. Chrome represents nearly 66% of the total global browser market share, so the impact is significant. Safari, Firefox, and other browsers have also ended or plan to end support.

While it may sound like a scary road ahead for advertisers, publishers are preparing to accommodate the change by modifying how they offer audience segments to advertisers. Some are even making the best of the situation by attempting to capture a higher share of ad revenue by eliminating third parties that take a cut.

Cookies 101

Cookies are used widely across the Internet. Continue reading to learn more about why advertisers love them while consumers are turned off.



What are cookies?

Cookies are small pieces of tracking code that get added to a user's web browser by either a website or a third party, often without the user's knowledge.

Why are they used?

There are different types of cookies. First-party cookies are used by a site owner to track what a user does while on the site and may offer helpful services like remembering login information, maintaining a shopping cart, or suggesting personalized content. Third-party cookies are commonly generated by ad servers and used to track consumer behavior across multiple sites for the purpose of selling highly targeted ads and measuring their performance.

What gets stored?

Cookies can capture everything from technical information like IP address, default preferences, and device type to highly personal data such as browsing history, search terms, religious beliefs, sexuality, health issues, and political conviction.

How do third-party cookies work?

Third-party vendors use cookies to supply ad servers with raw personal data to predict user behavior. Advertisers then purchase those predictions in real-time bidding auctions that ultimately lead to personalized ads on websites.

Why are third-party cookies going away?

Regulators and other organizations want to give users increased control over their personal data and how it's used. Cookies can be used to create a highly personal user profile that can be sold to advertisers — often without the user's consent. For example, based solely on browser and search history, an advertiser could identify a user as an overweight diabetic man in his 50s who's interested in hair replacement.

What publishers are doing about it

Publishers are exploring alternatives that take into account the increased needs of users to manage their privacy while still offering the advanced tracking required by advertisers. Here are a few of the leading solutions:

Zero-party data

Zero-party data is information that is explicitly shared by a user with a website. The method of collection typically includes setting preferences, selecting specific topics of interest, or opting in to receive certain content. Publishers that require subscription or registration are able to collect this data and use it to create a more personalized service. Because users are actively providing this personal data, they are aware of the information being supplied and can change or remove it.

First-party data

Many publishers have developed proprietary systems to use the data they collect from and about users, also known as first-party data. This requires a large scale to shape high-volume audience segments that are appealing to advertisers. The approach can result in a higher percentage of revenue for publishers because third parties are no longer taking a cut.

Ultimately, the success of this approach will depend on the value advertisers place on a publisher's audience.

The New York Times

The New York Times offers dozens of audience segments to advertisers based on first-party user data such as age, income, and interest.

The Washington Post

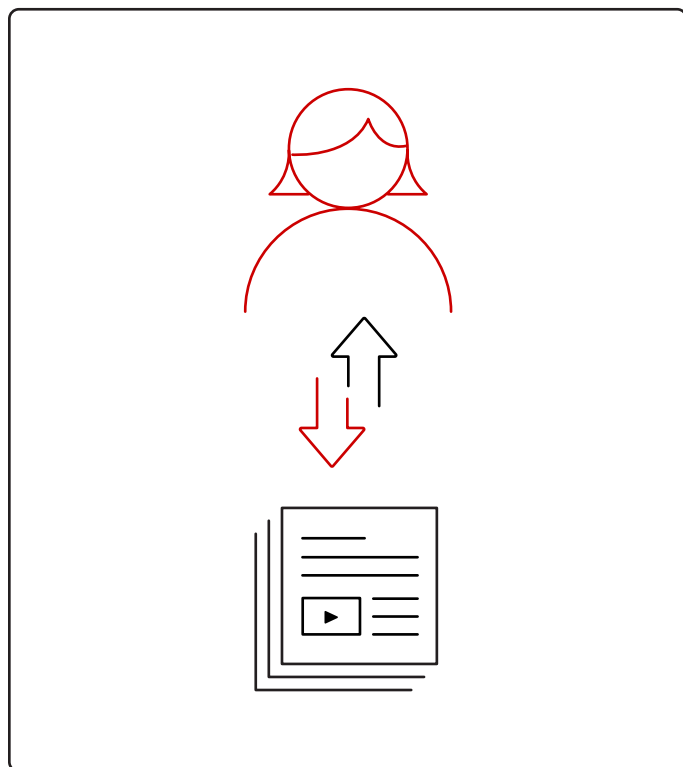
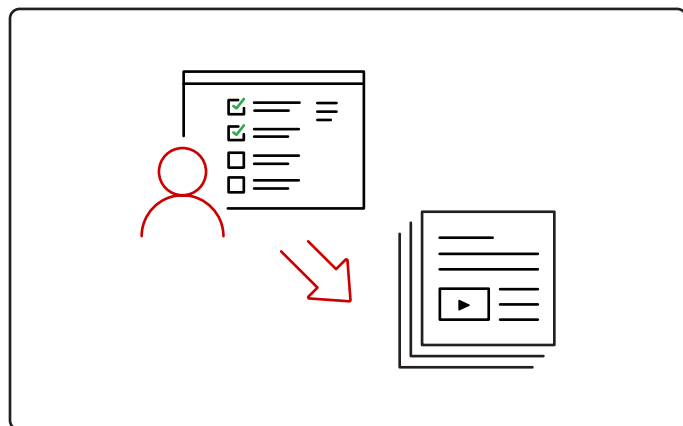
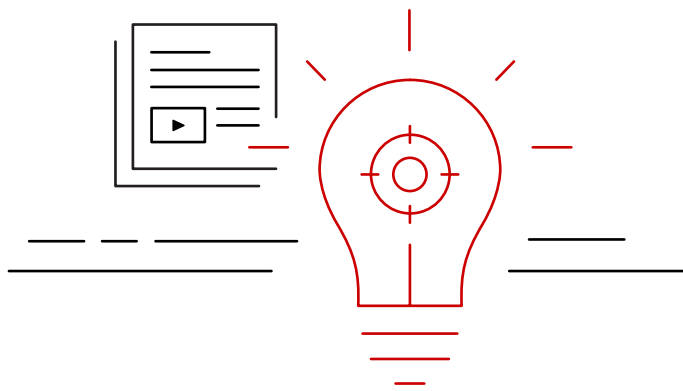
The Washington Post has developed its own ad network platform based on first-party data and has opened it up to outside publishers to join in order to create greater scale for smaller publishers.

VOXMEDIA

Vox Media recently launched an initiative named Forte to enable targeted advertising based on user data collected within the Vox Media network of sites.

News Corp HEARST BuzzFeed meredith

Many other publishers such as News Corp, Hearst, BuzzFeed, and Meredith are also engaged in optimizing their first-party data.



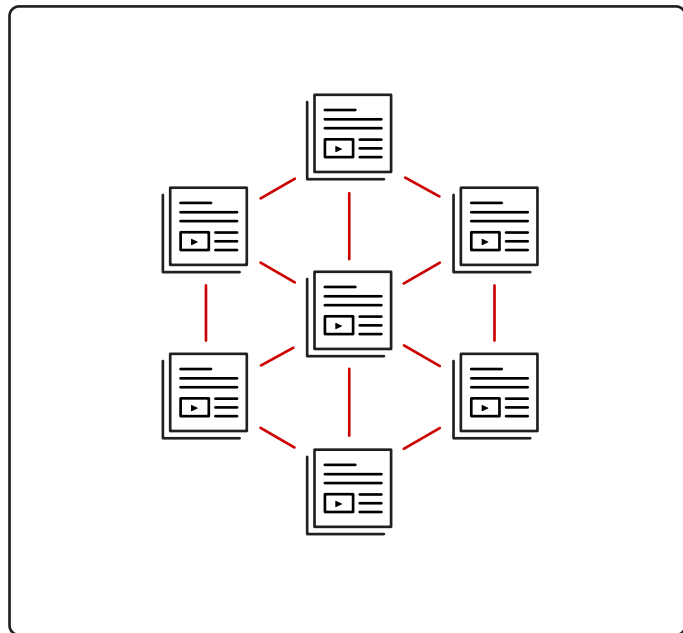
Advertising alliances

Alliances have been formed between TV networks and publishers to serve targeted ads to both linear television and digital platforms. Audience segment definitions are shared across publishers in the alliance, delivering the scale that advertisers seek. Examples include:

OpenAP AMC Networks, FOX, NBC Universal, Viacom CBS, Univision, and The Weather Channel

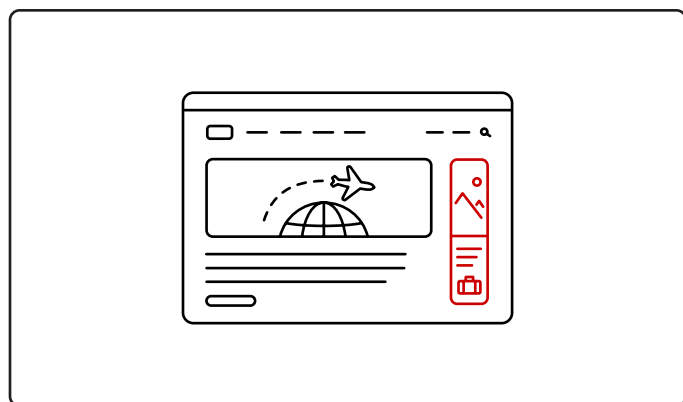
AdSmart Global, national, local TV and streaming content from NBC Universal

Viacom CBS eyeQ Global, national, local TV and streaming content from Viacom CBS



Contextual ad targeting

Rather than relying on personal data about users, advertisers can target users based on content found on the page they are viewing. For example, if a user is reading a story about the top ten travel deals this year, they may see an ad from a resort at one of those destinations. This approach doesn't give advertisers the sophistication or depth of targeting they have come to appreciate, but it does enable some targeting at scale.



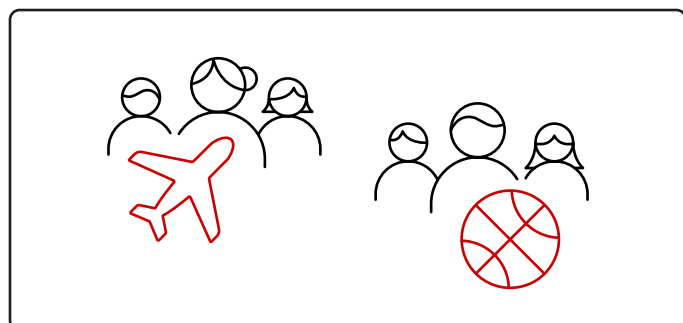
Digital fingerprint

While this technique does not contain personal information, it communicates device-centric information to a website that creates a unique user profile. The profile may include IP address, time zone, installed plugins, and operating system details that can be used for targeted advertising. It enables targeting but insulates user interests.



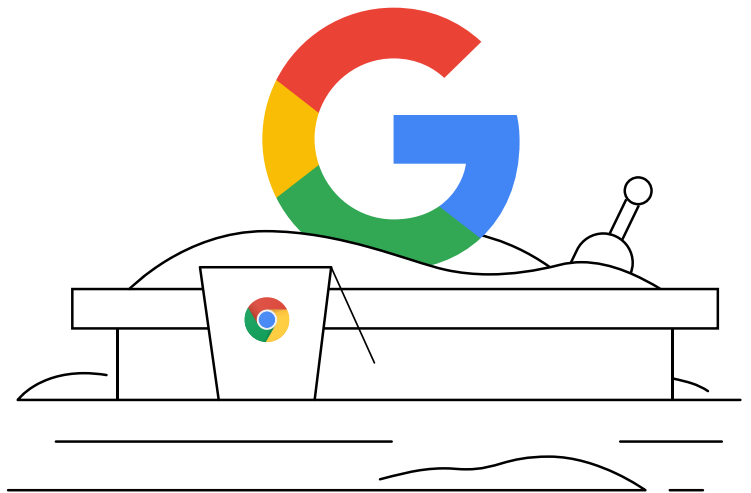
Unified audience segments

There are efforts underway by ad network companies and others to define a universal set of audience segments based on publisher-supplied first-party data. Standardized segment definitions would enable advertisers to reliably target consumers across the internet. The challenge is to define segments in a meaningful way for both publishers and advertisers.



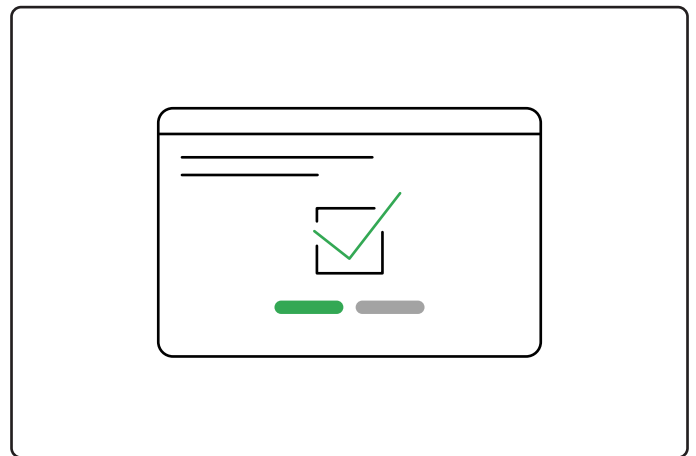
What Google is doing about it

Because the change could greatly impact Google's bottom line, the company is developing new solutions to address the needs of publishers, advertisers, and users. Its toolset, Privacy Sandbox, is in a draft state and will continue to be defined over the coming months. Chrome engineering director Justin Schuh wrote, "Some ideas include new approaches to ensure that ads continue to be relevant for users, but user data shared with websites and advertisers would be minimized by anonymously aggregating user information, and keeping much more user information on-device only."



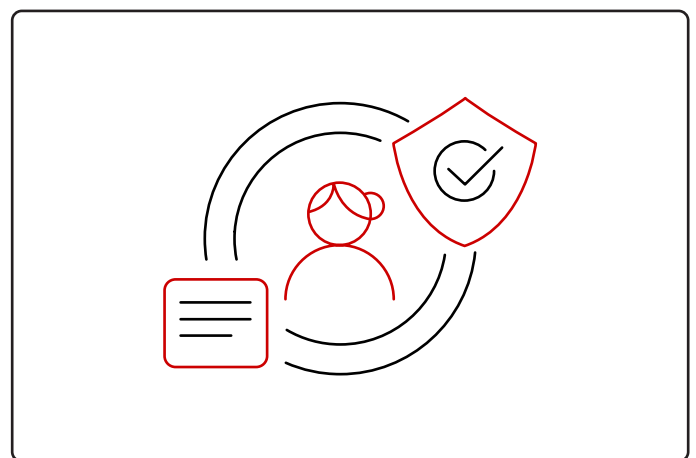
Google consent mode

Google launched Consent Mode in September 2020. This gives a user the option to let websites collect non-identifying aggregate user data to display more targeted advertising if the user decides not to consent to third-party cookies.



Trust tokens

One Google proposal is to replace third-party cookies with "trust tokens." These tokens would confirm that a user is real and use personal data to aggregate them into groups of interest, such as men with arthritis or female homeowners. Advertisers would then bid on and purchase groups, similar to how it works today. Tokens would not be operated by third-parties, but they could contain sensitive personal data and therefore will require consent on the part of users.

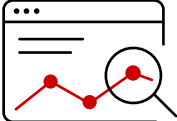


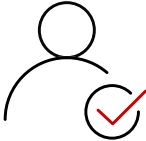
The takeaway

The key is leveraging owned, first-party data to drive ad revenue while balancing it with user consent.

Large publishers, like NBC Universal, may have a network of owned sites that provide enough scale to use only their own data. Smaller publishers may need to join an alliance with other publishers to form their own “ad network” based on shared first-party data. Many

publishers will use a combination of the alternatives listed above to capture as much revenue as possible. No matter the solution, publishers should consider these steps:

1  Understand the first-party data that is currently collected and determine if there are opportunities to expand that data.

2  Examine existing customer data collection and consent models to ensure these three requirements are addressed:

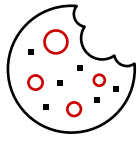
Consent Users must have a way to give consent for their data to be stored by a site or browser. Consent will need to be renewed regularly and when changes are made to data usage.	Inform Users must be notified about how their data is being collected, stored, and used.	Change or Remove Users must be given a mechanism for changing or deleting the data they have provided.
--	--	--

3



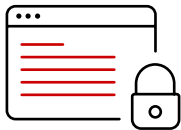
Invest in a Consumer Data Platform (CDP) to help collect, store, and analyze customer data. Consider investing in a Consent Management Platform (CMP) to handle user consent updates.

4



Begin switching from third-party cookies to first-party cookies.

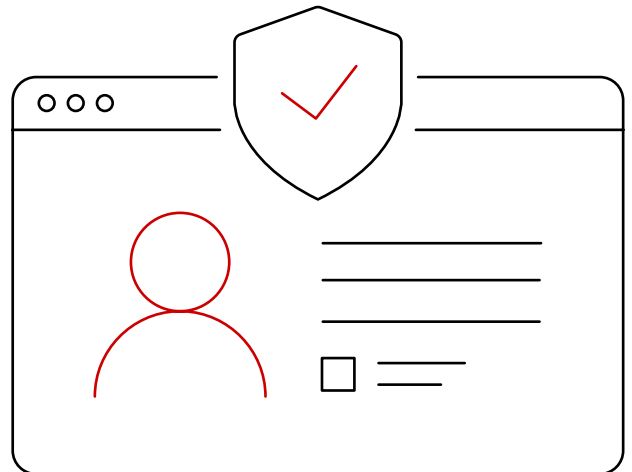
5



Ensure privacy policy pages are updated with current practices.

Giving consumers control over their personal data forms the backbone of the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR) in Europe. U.S. trends indicate that the handling of personal data will continue to move in this direction.

While Google is a driving force behind the end of third-party cookies, the entire ad industry is working towards a standardized means of targeting users with ads and measuring their effectiveness. We don't yet know which approaches will ultimately succeed, but publishers should take action now for the inevitable changes ahead.



CNN Newsource understands what it takes to win in the digital space. We work closely with our network of 1,000+ local news partners to offer valuable insights relevant to the news business while providing powerful, trusted news content.

