# Beyond Third-Party Cookies

## Your Guide to Privacy-Friendly Advertising

Basis® Technologies

# TABLE OF CONTENTS

# Introduction

The deprecation of third-party cookies—and other matters related to privacy—will continue and are inevitable as the focus on user data collection and sharing persists for the foreseeable future among regulatory bodies, browser developers, and operating system owners.

Most of the conversations around ad tech focus on a single direct impact area: the cookie-based audience targeting for demand side platforms (DSPs). Although it is the most visible one, there are other use-cases impacted by identity changes, primarily, frequency capping and attribution. The problem extends beyond DSPs to search and social buying platforms, affecting virtually all ad tech providers.

What this means for the industry is a reimagining of how the impacted use-cases can be brought forward in a privacy-friendly manner. Audience targeting will continue, but with a significantly heavier reliance on contextual targeting than in the past. Where brands are well-positioned in capturing first-party data, most publishers are laggards; however, we expect publishers to begin to place higher importance on the capture and utilization of this data as the impact becomes more real. This presents an opportunity for companies that are well-positioned between the two to provide services that allow for greater fidelity in identifying overlapping populations to help guide the allocation of media spending from brands to publishers who speak to a higher population of the brands' desired audience for a particular campaign or initiative.

# How did we get here?

As new technologies have emerged, so has the public and private interest in how and why ads are being shown to consumers. Tracking methodologies that allow advertising technology suppliers to create targeting mechanisms have been the subject of scrutiny for the last decade. In response, technology developers and regulatory bodies have stepped in to protect and enforce users' right to privacy and choice.

## TIMELINE OF CHANGE

### 2003
CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act)

### 2010
US Federal Trade Commission (FTC) publishes preliminary report on consumer privacy rights

### 2016
General Data Protection Regulation (GDPR) adopted by the European Union

### 2017
Apple Intelligent Tracking Prevention (ITP) limiting tracking on Safari

### 2018
Mozilla Enhanced Tracking Protection (ETP) released limiting trackers and third-party cookies on Firefox browsers

GDPR goes into effect

California Consumer Privacy Act (CCPA) passed into law

### 2019
Microsoft Tracking Prevention (MTP) blocks third-party cookies on its browsers

Apple Intelligent Tracking Prevention (ITP) is enhanced to block all third-party cookies in Safari by default

### 2020
California Consumer Privacy Act (CCPA) goes into effect

### 2021
Apple iOS14.5 prompts users to opt-out of tracking, reducing the availability of IDFAs

Virginia Consumer Data Protection Act (CDPA) is signed

### 2023
California Privacy Rights Act (CPRA) and four other state-level data privacy laws go into effect.

### 2024
Google Chrome blocks third-party cookies by default [PENDING]

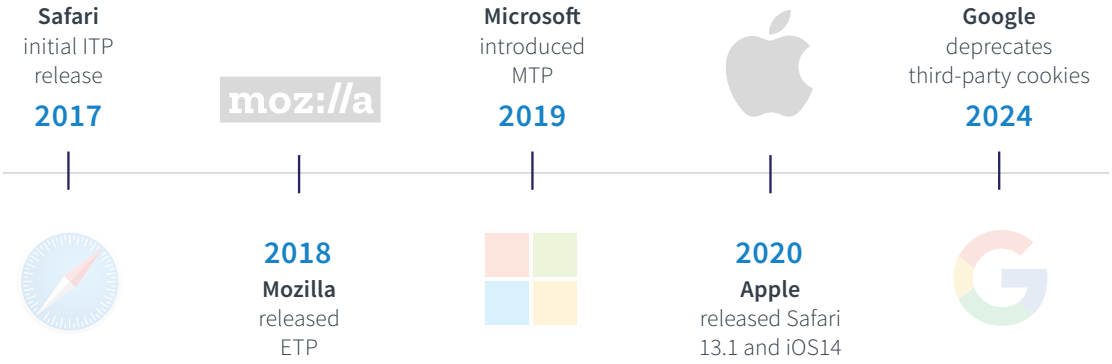
# TECHNOLOGY DEVELOPERS

In 2018, Mozilla released Enhanced Tracking Protection (ETP)—a setting that allowed Firefox users to block third-party cookies[1]. A year later, the company made changes so ETP would only block known trackers and not all cookies; Mozilla found that blocking all cookies "leads to scenarios where some websites may not function properly," therefore took this modified approach to prevent "potential usability issues." Users who prefer more protection and privacy can change the tracking settings from the default "standard", to "strict". [2]

Microsoft followed suit, and in 2019 introduced Microsoft Tracking Prevention (MTP). Like Mozilla's ETP, MTP offers users multiple protection levels: basic, balanced (the recommended and default option), and strict. MTP blocks third-party cookies from known tracking sites, and in strict mode, blocks calls to those sites. Unlike ETP, Microsoft does not offer a custom mode and doesn't behave differently between InPrivate or normal browsing.

With the release of Safari 13.1 in March 2020, and through updates to the Intelligent Tracking Prevention (ITP) privacy feature, Apple now blocks all third-party cookies in Safari by default. [3] With the release of iOS14, Apple gave users a prompt to opt-out of tracking, thus reducing the availability of IDFAs—the Identifier for Advertisers is a random device identifier assigned by Apple to a user's device. Advertisers use this to track data so they can deliver customized advertising.

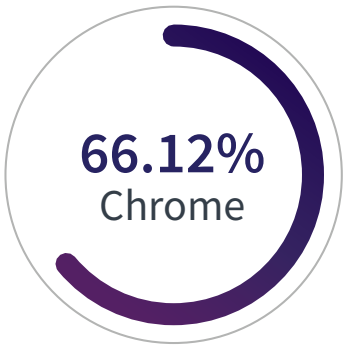
## PRIVACY TIMELINE



In 2020—in response to users' demand for greater privacy, including transparency, choice, and control over how their data is used—Google announced its intentions to phase out support for third-party cookies in Chrome. Later that year, they introduced Privacy Sandbox as the home of its effort to "make the web more private and secure for users, while also supporting publishers."[6] Google has since delayed the deprecation of third-party cookies on Chrome two times since the initial announcement, now saying the phase out will begin in the second half of 2024.

To fully appreciate the impact of Google's decision to deprecate third-party cookies in Chrome, it helps to look at the numbers for browser market share:

## BROWSER MARKET SHARE

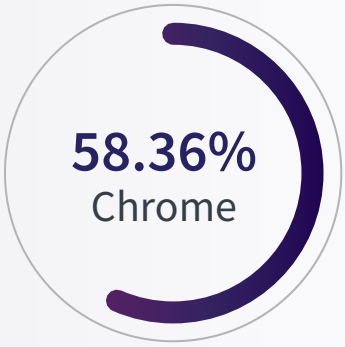


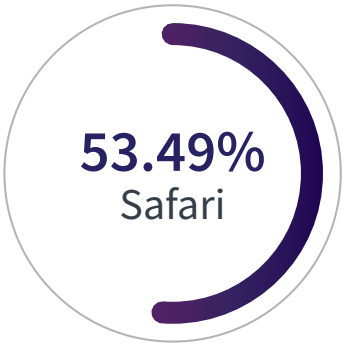

### BROWSER USER MARKET SHARE (DESKTOP/WORLDWIDE) - MAR 2023[7]

Chrome: 66.12%
Safari: 10.14%
Firefox: 6.84%
Edge: 10.84%
Opera: 3.21%
360 Safe: 0.83%

### BROWSER USER MARKET SHARE (DESKTOP/USA) - MAR 2023[8]

Chrome: 58.36%
Safari: 19.33%
Firefox: 6.22%
Edge: 13.23%
Opera: 1.68%
IE: 0.50%




### BROWSER USER MARKET SHARE (MOBILE/USA) - MAR 2023[9]

Chrome: 41.67%
Safari: 53.49%
Firefox: 0.95%
Samsung: 3.41%
Opera: 0.56%
Edge: 0.3%

# REGULATORY BODIES

In recent years, governments in Europe and North America have been developing laws to protect consumers' data privacy rights. Europe's stance has been stricter by creating an opt-in system, whereas North America has started with an opt-out approach—the default assumption between the two are significant.

In 2016, the European Union approved the General Data Protection Regulation (GDPR), which was put into effect in May 2018. The regulation governs the collection and processing of personal data of European member state citizens (data subjects). Under GDPR, personal data that is used to offer goods and services, or to profile users, can only be collected for explicit, specified purposes, and the processing of that data must be compatible with those same purposes.

There are only a few very specific legal bases for processing, most notably, through the consent of the data subject. In addition, data subjects have very broad rights, including the right to transparent information about the data collection and processing, the right to be forgotten (erasure of data), the right to object, and others. The intention of the regulation is to give data subjects more control over their personal data: who can use it, how it is used, who it can be shared with, etc. All companies that interact with European end-users are obligated to comply with this law regardless of said companies' geographic location. Therefore, advertisers need to ensure that their advertising activities are lawful under the GDPR when targeting EU member states in their campaigns. Advertisers that collect and process personal data, and have determined that their activities fall within GDPR's scope, need to be certain they have a valid legal basis (such as user consent) for doing so.[11]

In 2022, the European Parliament passed the Digital Services Act (DSA) and Digital Markets Act (DMA). Transparency provisions in the DSA are intended to help users better understand how platforms moderate their content and recommend it to them, while the DMA will require gatekeepers to provide business users with access to data related to the use of their services as well as to advertising performance data. The new laws will compel social platforms to dedicate more resources to preventing misinformation and hate speech on their platforms and ban any targeted online ads that are based on an individual's ethnicity, religion, or sexual orientation. Google, Meta, and Amazon advertising will also have to abide by the new rules set in place as well as possible annual audits. [13]

Privacy regulations also came to the US, notably, the California Consumer Privacy Act (CCPA) which was signed into law in June 2018 and became effective in 2020. CCPA gives California residents new rights regarding their data – regardless of if they are in California or not, including: the right to know about the personal information a business collects about them and how it is used and shared; the right to delete personal information collected from them (with some exceptions); the right to opt-out

of the sale of their personal information; and the right to non-discrimination for exercising their CCPA rights.[14] Building upon the CCPA right to request access to the personal information a business has collected about a person in the preceding 12-month period, the California Privacy Rights Act (CPRA) expands this to include any information collected—regardless of when it was collected—unless doing so proves impossible or would involve a disproportionate effort. CPRA went into effect January 2023.[15]

# IMPACT OF THIRD-PARTY COOKIE DEPRECATION

Advertisers have used third-party cookies for things like audience targeting, retargeting, geo-based retargeting, cross-device targeting and tracking, and frequency capping. Additionally, cookies can facilitate a variety of attribution—a measurement of return on ad spend—such as foot traffic/walk-ins, click-through conversions, and view-through conversions. While all these functions will be impacted by third-party cookie deprecation, the biggest disruption to advertisers will be losing the ability to measure view-through conversions and large-scale third-party audience segments.

Not all aspects of digital advertising will be impacted equally. Most advertising on connected TV (CTV) and on mobile occurs within apps, making third-party cookie deprecation less of a problem for these devices. Similarly, most ad verification does not need to rely on cookies to detect fraud, deliver brand safety or measure viewability, so verification solutions should be able to continue as usual.

### Advertisers

Limitations in campaign tactics & personalization

### Consumers

Less relevant, personalized online experiences

### Regulators

Legislation to limit potential misuse of collected user data

### Browser/OS

Limiting or blocking certain tracking IDs and/or cookies

### Publishers

Reduced revenue opportunities and pricing model shifts

## IT'S NOT ALL BAD

Regain consumer trust and operate more sustainability

More privacy online and greater control over their data

Limit privacy violations and increase trust in the online ecosystem

Create a more secure and enjoyable environment for users

Opportunity to monetize first-party data

# Identity Solutions for the Industry and Basis

The digital media ecosystem is a dynamic one, with new methodologies, systems, and opportunities emerging every day. Advertisers are looking for a better way forward—one that embraces change without sacrificing performance. That is why Basis created BasisConnect+.

BasisConnect+

- Connect with Consumers
- Run and Measure Impactful Media

# PRIVACY-FRIENDLY SOLUTIONS FROM BASISCONNECT+

## Resources for creating sustainable advertiser/consumer connections for an evolving digital ecosystem:

- First-Party Data: Basis Technologies is actively implementing solutions that allow both marketers and publishers to better leverage their first-party data in their digital advertising efforts. One example: through a partnership with LiveRamp, Basis converts a user's CRM data into targetable first-party audience segments within minutes.
- Look-a-Like Modeling: Another great way to leverage first-party data, look-a-like modeling uses what you already know about your existing customers to identify and build new pools of prospects that resemble them—and have a higher likelihood of converting. Basis partners with TransUnion to enable look-a-like modeling through the use of CRM uploads or site-pixel data.
- Audience Targeting: Through integrations with premium specialists in the market—including Comscore, DoubleVerify, Oracle, and Peer39—Basis users can access hundreds of segments that align their ads next to the most relevant content. Targeting options are available for popular categories such as demographic characteristics, location, interests, or page ranking. To facilitate optimal segment selection, Basis offers a one-of-a-kind, privacy-compliant cookieless targeting solution that automatically recommends contextual categories based on a marketer's best performing audiences.
- Leverage AI: Basis uses artificial intelligence and privacy-approved data across 30 parameters to decide if and how much to bid on an impression. This tactic can improve media performance without relying on cookies or infringing on the audience's privacy—and, when paired with bid shading, helps users purchase inventory at the optimal price.
- Incorporate Semantic Targeting: Contextual targeting has come a long way over the last decade and now uses Natural Language Processing to understand semantics and tone. Basis partners with semantic data providers such as comScore, DoubleVerify, Grapeshot, and Peer39. (And guess what? Semantic data is more affordable than third-party audience data!)

# PRIVACY-FRIENDLY SOLUTIONS FROM BASISCONNECT+ *(CONTINUED)*

- Cookieless Conversion Tracking: Basis has updated tracking technology that allows users to measure cookieless click-through conversions, empowering advertisers to fulfil standard campaign management activities such as performance tracking/reporting and helping maximize return on ad spend.
- Anonymized Data Sources: Expanding ingestion of anonymized data sources for improved fidelity of local data in aggregate is key to continuing to drive smarter decisions in a post-cookie world. Utilizing data sources like the US Census, American Community Survey and North American Industry Classification System provide a robustness to local insights and allow for smarter decisions and improved performance.
- Premium Inventory: With buying methods such as site direct, connected TV, private marketplace deals and programmatic guaranteed—all of which are available to Basis users—advertisers can ensure media placements in front of desired audiences without having to rely upon third-party cookies.

# INDUSTRY IDENTITY SOLUTIONS

To prepare for a future without cookies, Basis Technologies has been closely watching and collaborating with other members of the industry. The success of an identity solution is heavily dependent on scale, and therefore partnering with an independent owner of a solution with the most scale, or partnering with multiple, is the option we are focused on. Working as a group, evaluating options, and sharing principles is the best course we can take to minimize the impact on our customers. Partners include LiveRamp's RampID and IAB Project Rearc. Partnering with these industry leaders is an important first step in providing privacy-centric and sustainable identity to our customers at scale. That said, there is still a lot to learn, and we are continuing to investigate industry solutions in order to provide the best possible solutions for a cookieless world.

## IAB PROJECT REARC //

In February 2020, the International Advertising Bureau (IAB) introduced Project Rearc, a global initiative designed to get stakeholders across the digital advertising and media supply chain together to re-architect digital marketing in a consolidated effort to harmonize personalization and consumer privacy. Along with other industry leaders, Basis Technologies has been an active participant in this project; reviewing the proposals, submitting comments, evaluating specs, and providing feedback.

It proposes rigorous technical standards and guidelines that inform how companies collect and use such an identifier so that[17] :

- Consumers are in control of the use of the ID and any related data. Any privacy preferences attached to the identifier are strictly followed.
- The identifier is sufficiently encrypted so that it cannot be reverse engineered to identify the person.
- Brands and publishers have auditable, technical assurances that third-party vendors cannot track consumers on this basis without explicit consent.
- Third-party vendors are able to execute on behalf of trusted first parties, without compromising any of the above objectives.
- Standardized consumer-facing messaging, and accountability mechanisms that ascertain responsible privacy practices.

## LIVERAMP RAMP ID //

LiveRamp, one of our long-term partners, manages the largest deterministic graph on the open internet, representing more than 250 million consumers around the US and many more across the globe. In 2016, LiveRamp introduced IdentityLink —now known as RampID—which allows resolving hundreds of different identifiers for consumers used on devices and marketing platforms in a privacy-compliant manner. It doesn't matter if data is offline or online, first-party CRM or third-party behavioral, online exposure data, or mobile app download data—all of it can be tied back to a unique, privacy-safe identifier at the consumer level.[18] Basis users can upload their CRM data directly into the platform. Without the need for any external tools or contracts, their files are processed securely by LiveRamp and converted into targetable segments. The automatic processing of the files makes these first-party segments available to marketers on the same day, which they can use to identify and model new audiences more effectively, activate data directly with publishers and platforms, or reach audiences programmatically.

# Conclusion

It's a new era for adtech, one filled with opportunity and room for innovation in the way we connect with our audiences.

Consumers' expectations and understanding of privacy rights are growing, and the private and public sector is responding to this. In the coming years, we can only expect for more laws, regulations, and protections to be put in place by governments, and for technology providers to transform their products to align with these requests.

Providing Raving Fan Service is in our DNA, we are committed to listening to the market, working with other industry members, collaborating with regulatory bodies, adapting and developing new products, and walking through the changes that this event brings with you.

# FAQs

### What is happening?

Google has communicated its intentions to phase out support for third-party cookies in its Chrome browser. While Google has repeatedly moved back the date upon which this move will take place, in July 2022, the company announced that it will occur in the second half of 2024.

### Why is this important?

Google Chrome represents approximately 70% of the browser market share, therefore marketers will have to leverage new tools to target users and measure the impact of their ads.

### Why is this happening?

Increased demand for privacy from users has led technology providers and governments to act. Firefox started blocking cookies in 2018 and the GDPR was approved in Europe in 2016. These are only two examples of how the industry has already been responding to users' concerns and honoring their wishes.

### Why are third-party cookies important?

They facilitate communication between websites and advertising technology. Primarily, they help advertisers target user segments, and track activity (conversions).

### What can advertisers do if they can't use third-party cookies to target users?

Popular tools advertisers can continue to leverage include PMPs, Machine Learning, and Contextual Targeting. These won't be affected by the deprecation of cookies.

### What about apps?

While mobile applications are not affected by changes to browsers, with the release of iOS14 in September 2020, Apple began giving users a prompt to opt out of tracking, thus reducing the availability of IDFAs. Advertisers use this to track data so they can deliver customized advertising.

### Are all platforms affected equally?

All buying platforms –DSPs as well as Search and Social platforms– will be impacted equally on conversion attribution. All DSPs will be impacted equally on third-party audiences. Private Marketplaces (PMPs) will not be impacted, in fact, we expect these to grow as publishers leverage their first-party audience data. Basis offers access to more than 1,700 pre-negotiated PMP deals.

### Is Basis Technologies developing a proprietary solution?

No. The success of an identity solution is heavily dependent on scale, and therefore partnering with an independent owner of a solution with the most scale, or partnering with multiple, is the path the company is taking.

### Is ad serving measurement expected to change in CM360 (formerly GCM)?

After the release of Safari ITP, Google unified its tagging infrastructure across its marketing platform (Google Analytics, CM360, Search Ads 360, Google Ads, YouTube, etc) with the release of the Global Site Tag and Event Snippet. This reduces its reliance on third-party cookies and instead sets a cookie on the client's domain. In cases where cookies are unavailable, Google also uses modeling to infer conversions based on observable signals in time/date/device, etc. The global site tag works in unison with another piece of code, an event snippet, or a phone snippet, to track conversions. To streamline the user experience by using website code across all Google products, users can use the global site tag to track Google Ads conversions. When users create a website conversion action in the new Google Ads experience, they see a global site tag instead of the previous conversion tracking tag. This tag should be installed on every page of a website. Users will also have to add another piece of code, an event snippet, or a phone snippet — depending on the type of conversion they want to track, to certain pages on a site. These snippets work in unison with the global site tag to track conversions.[19]

### Are there any specific updates on how Facebook will have to adjust to these changes?

In response to browser changes, such as Safari ITP and others, Facebook allows users to leverage first-party cookies. This has been available since 2018. Additionally, Facebook supports “Advanced Matching”, which allows marketers to pass other data (such as hashed emails, phone numbers, and so on) to improve user attribution. Beyond the browser, they also support S2S (server to server) tracking. This allows marketers to count events from their server when an event is initiated vs. relying on scripts firing in the browser. In response to IOS14, Facebook is also rolling out changes to their SDK (for app advertisers) and how/when pixel events (for web) will be recorded in Events Manager. More information will follow on this.[22]

### How will in-store foot traffic measurement be adjusted?

We expect the critical fundamental location data to decline as device-ids gradually decline in availability due to privacy changes by iOS first, then by Android. There is a possibility that a level of data remains, perhaps through incentives that app providers or data providers offer to consumers in exchange for sharing location data, but that remains to be seen.

# References


01 // The Verge, 2018 - *https://www.theverge.com/2018/10/23/18015234/mozilla-firefox-quantum-63-vpn-enhanced-tracking-protection*

02 // The Verge, 2018 - *https://www.theverge.com/2018/10/23/18015234/mozilla-firefox-quantum-63-vpn-enhanced-tracking-protection*

03 // ZD Net, 2020 - *https://www.zdnet.com/article/apple-blocks-third-party-cookies-in-safari/*

04 // The Verge, 2020 - *https://www.theverge.com/2020/3/24/21192830/apple-safari-intelligent-tracking-privacy-full-third-party-cookie-blocking*

05 // The Verge, 2020 - *https://www.theverge.com/2020/3/24/21192830/apple-safari-intelligent-tracking-privacy-full-third-party-cookie-blocking*

06 // Chronium Blog, 2020 - *https://blog.chromium.org/2020/01/building-more-private-web-path-towards.htmll*

07 // Stat Counter, 2023 - *https://gs.statcounter.com/browser-market-share/desktop/worldwide*

08 // Stat Counter, 2023 - *https://gs.statcounter.com/browser-market-share/desktop/united-states-of-america*

09 // Stat Counter, 2023 - *https://gs.statcounter.com/browser-market-share/mobile/united-states-of-america*

10 // IAB Europe, 2021 - *https://iabeurope.eu/wp-content/uploads/2021/02/IAB-Europes-Updated-Guide-to-the-Post-Third-Party-Cooke-Era-February-2021.pdf*

11 // Basis Technologies, 2018 - *https://www.centro.net/blog/guide-to-gdpr*

12 // European Commission, 2022 - *https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package*

13 // Shaping Europe's Digital Future, 2022 - *https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package*

14 // State of California Department of Justice, 2021 - *https://oag.ca.gov/privacy/ccpa*

15 // Privacy Rights Clearinghouse, 2020 - *https://privacyrights.org/resources/california-privacy-rights-act-overview#:~:text=The%20California%20Privacy%20Rights%20Act%20clarifies%20that%20people%20can%20opt,does%20not%20explicitly%20include%20sharing*

16 // Forrester, 2021 - *Programmatic Advertising Spend Key Trends (Report from Anthony) < does this need a link?*

17 // IAB, 2020 - *https://www.iab.com/blog/project-rearc-an-industry-collaboration-to-rearchitect-digital-marketing/*

18 // LiveRamp, 2016 - *https://liveramp.com/blog/introducing-liveramp-identitylink/*

21 // Google Ads Help, 2021 - *https://support.google.com/google-ads/answer/7548399?hl=en*

22 // Facebook for Business, 2021 - *https://www.facebook.com/business/help/611774685654668*

basis.com