Beyond Third-Party Cookies

Your Guide to Overcoming the Identity Crisis

Basis® Technologies

TABLE OF CONTENTS

A NOTE FROM BASIS' FOUNDER AND CEO //

Embracing the “Identity Crisis” – Basis Technologies’ Perspective

To my industry friends, colleagues, and competitors,

This is not the end. It’s not doomsday. I believe this is an opportunity. We are an industry filled with innovators, optimists, and consumer-centric problem-solvers. Advertising was around long before the cookie and it will be here long after.

There’s no need to panic. Instead, let’s focus on the two sides of the equation, our industry’s main stakeholders: marketers and consumers.

For **marketers and advertisers**, the deprecation of third-party cookies brings questions, mostly surrounding targeting and performance. How will I reach my target? How will I know my media is working and measure conversions? I address these questions below and this guide goes further in-depth into your options.

Consumers, on the other hand, are sending a message—they are telling us that privacy matters and they need to be in control. Many solutions being proposed and developed by organizations in the advertising industry are not respecting this—these solutions are just exploiting loopholes and replacing one problem with another. We need to honor the spirit of privacy and find a real solution.

It’s important to note that this challenge is not unique to Basis Technologies. We are a proud active participant in groups working toward a solution, specifically Project Rearc, the IAB’s working group addressing privacy changes.

I understand that the impending changes to cookies will probably arrive before a true Identity solution can be built.
So, what now? What can we do in the near term? We have options for reliable targeting and alternative reporting options.

- **First-Party Data.** With improved efforts by brands and publishers to collect customer first-party data in order to create more customized user experiences, the question becomes how can each use that data to make smarter decisions outside the walls of their owned and operated properties. As a partner to both marketers and publishers, Basis Technologies is actively working on solutions that allow for anonymized overlap analysis between both parties. One recent example: through a partnership with LiveRamp, Basis converts a user’s CRM data into targetable first-party audience segments.
- **Leverage Machine Learning.** Best-in-breed solutions will leverage machine learning technology that 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 all without the use of cookies or infringing on the target’s privacy—and, when paired with our bid shading algorithm, helps users purchase inventory at the optimal price.
- **Incorporate Semantic Targeting.** Targeting has become synonymous with audiences over the years of programmatic buying, and much of the audience buying world is cookie-based and deprecating. This doesn’t mean your targeting needs to suffer—you have many other compliant targeting options. Contextual targeting has come a long way over the last decade and now uses Natural Language Processing to understand semantics and tone. We've chosen to partner with semantic data providers such as, comScore, DoubleVerify, Grapeshot, and Peer39. And guess what? Semantic data is more affordable than third-party audience data.
- **Leverage reporting.** Placing ads alongside precise, targeted content is critical to the success of a campaign. Tools like our Contextual Insights Report can show media buyers the segments that are generating the most actions. With this knowledge, buyers can make changes to their tactics and optimize accordingly.
- **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 sources of data such as US Census, American Community Survey and North American Industry Classification System provide a robustness to local insights, and allow for smarter decisioning (both machine learning and manual) to improve performance and eliminate wasted impressions.
- **Performance Tracking.** Individually and as an industry, we are working on revamping our solution for performance tracking, particularly for actions taken on advertisers’ websites. We’ve updated our tracking technology to allow you to measure click-through cookieless conversions. In the mid-term, the most reliable way to understand the full impact of a campaign will be through a combination of cookieless conversion tracking, Consumer Data Platform (CDP) records, site analytics data, and brand lift studies. This is a shiftfrom only using conversion tracking but can more fully and thoughtfully illustrate media performance.

And for that long-term vision mentioned earlier, this is an opportunity—an opportunity to address the real problem, an opportunity to tell stories, an opportunity to be better as an industry. Some companies are trying to find loopholes and circumvent the legislation. Even if they find success, it will be short-lived. They are ignoring what consumers are saying. These players need toaddress the problem and create solutions that are good for our ecosystem and respect the rising concern for data privacy.

With optimism and excitement,

Shawn Riegsecker
Founder & CEO of Basis Technologies

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.

EMBRACING THE IDENTITY LANDSCAPE //

How did we get here?

Digital advertising has come a long way from the first display ad in 1994. 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 eight years. In response, technology developers and regulatory bodies have been acting in protecting and enforcing users' right to privacy and choice.

TECHNOLOGY DEVELOPERS

In 2018 Mozilla released Enhanced Tracking Protection (ETP)—a setting of Firefox 63 that allows 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] According to John Wilander, Security & Privacy Engineer at WebKit (Apple), "This is a significant improvement for privacy since it removes any sense of exceptions or 'a little bit of cross-site tracking is allowed,'".[4] Wilder explains that users are unlikely to notice any changes because ITP has already been doing some of this for several years, "It might seem like a bigger change than it is. But we've added so many restrictions to ITP since its initial release in 2017 that we are now at a place where most third-party cookies are already blocked in Safari."[5] 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

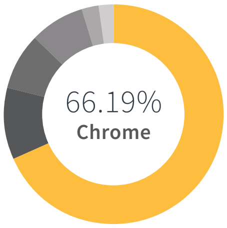
Safari initial ITP release	Mozilla released ETP	Microsoft introduced MTP	Apple released Safari 13.1 and iOS14	Google deprecates third-party cookies
2017	2018	2019	2020	2024

Google Chrome communicated its intentions to phase out support for third-party cookies through a blog post in January 2020 and public comment within the Web Advertising Business Group opened to define alternatives. In August 2020, Google announced Privacy Sandbox, as a response to users' demand for greater privacy—including transparency, choice, and control over how their data is used. Google's stance is that simply allowing users to change their privacy settings isn't enough, and that can lead to unintended negative impacts on users and the web ecosystem, encouraging practices such as fingerprinting, which can reduce user privacy and control. The goal of Privacy Sandbox is "to make the web more private and secure for users, while also supporting publishers."[6]

Understanding the impact of Google's choice is facilitated by looking at each browser's share of the market across the globe, and the US, specifically.

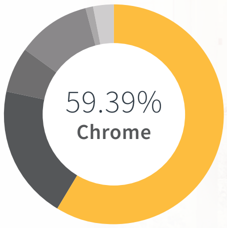
BROWSER MARKET SHARE

BROWSER USER MARKET SHARE (DESKTOP/WORLDWIDE) - AUG 2022[7]



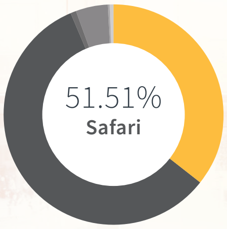
Chrome: 66.19%
Safari: 8.94%
Firefox: 8.08%
Edge: 10.84%
Opera: 3.06%
IE: 0.75%

BROWSER USER MARKET SHARE (DESKTOP/USA) - AUG 2022[8]



Chrome: 59.39%
Safari: 16.54%
Firefox: 6.85%
Edge: 14.14%
Opera: 1.62%
IE: 0.76%

BROWSER USER MARKET SHARE (MOBILE/USA) - AUG 2022[9]



Chrome: 42.41%
Safari: 51.51%
Firefox: 0.84%
Samsung Internet: 4.45%
Opera: 0.45%
Edge: 0.26%

> Already, we've been operating in an environment in which 30% of impressions aren't reachable through third-party cookie-based audiences, and their response to campaigns has not been fully measured either.

Marketers have already been successfully applying tactics to reach those consumers, and any conversion performance is already under-represented due to attribution being blocked. Cookieless conversions will automatically increase click-through conversions on these other browsers that are currently locked out. As Chrome accounts for approximately 70% of the remaining browser usage, its impending change threatens cross-publisher-based advertising.[10]

REGULATORY BODIES

Browsers aren't the only ones who have been reacting to users' demands; governments in Europe and North America have been developing laws to protect consumers' data. 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 goes into effect January 2023.[15]

IMPACT OF THE THIRD-PARTY COOKIE

A third-party cookie is a piece of code set by a website other than the one a user is currently on. This snippet of code is primarily used to identify and track visitors between websites and display more relevant ads. These cookies help media buyers execute popular techniques, so their ads are shown to the right person, in the right environment, at the right time, including audience targeting, retargeting, geo-based retargeting, cross-device targeting and tracking, and frequency capping. Additionally, cookies facilitate a variety of attribution—a measurement of return on ad spend—such as foot traffic/walk-ins, app installs, and conversions via click-through and view-through. While all these functions will be impacted, the inability to measure view-through conversions will present the biggest disruption to advertisers because of its ubiquity across the industry. Third-party audience segments will also be impacted by the loss of third-party cookies, but they will still exist though at a smaller scale; the exact time it will take for these to be fully phased out is undetermined as it will depend on how long it takes for users to adopt the new version of Chrome.

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; verification solutions will therefore be able to continue as usual.

PRIVACY TIMELINE

<table>
<tr><th>Environment</th><th>Browser / Operating System</th><th>Conversion attribution</th><th>Third-party audience targeting</th><th>Audience targeting by publishers on own site/apps</th></tr>
<tr><td rowspan="3">Web</td><td>Chrome</td><td colspan="2">Not supported</td><td>Supported</td></tr>
<tr><td>Firefox</td><td colspan="2">Not supported</td><td>Supported</td></tr>
<tr><td>Safari</td><td colspan="2">Not supported</td><td>Supported</td></tr>
<tr><td rowspan="2">App</td><td>Android</td><td colspan="2">Supported for now</td><td>Supported</td></tr>
<tr><td>iOS</td><td colspan="2">Expected drop by the end of 2021</td><td>Supported</td></tr>
</table>

EMBRACING THE IDENTITY CRISIS //

Innovating Solutions for the Industry and Basis

The digital media ecosystem is a dynamic one, with new methodologies, systems, and opportunities emerging every day. The third-party cookie has been a protagonist in the last 20 years, but it's not the only character in this story.

Since its inception, Basis Technologies has been establishing partnerships and developing products to empower high-performing marketers with the world's most automated and comprehensive advertising platform. Our technology and people meet you where you are and take you where you want to go. For over two decades we've been finding solutions to bind a fragmented space, the deprecation of cookies is another chapter we are prepared for.

Basis offers contextual solutions for desktop, mobile, and CTV. Through integrations with premium specialists in the market—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, interests, or page ranking. To facilitate selecting segments, Basis offers a privacy-compliant, one-of-a-kind cookieless targeting solution. The feature, powered by Peer39, automatically recommends contextual categories based on a marketer's best-performing audiences.

To make the most of contextual targeting, advertisers should consider:

- Tactical terms—what words can lift their KPIs?
- Brand protection
- Building custom contextual segments that align with their individual campaign objectives, leveraging partners that can help automate segments in real-time
- Utilizing the Basis suite of optimization solutions, which includes Bid Shading, Machine Learning, Algorithmic Optimization, Bid Multipliers, and Group Budget Optimization

Together, these tactics can help maximize campaign performance. Private marketplace deals (PMPs) are another solution marketers and publishers should continue to take advantage of. PMPs are customized, invitation-only RTB marketplaces where premium publishers make their inventory and audiences available to a select group of buyers. Basis' PMP library – curated by a team of specialists– contains over 2,000 deals for users to choose from, each with an analytics card, providing details about the deal, auction breakdown by geographic location, and auction volume by device and ad size. As cookie-based audiences decrease in size, Publishers can and should leverage their first-party data and make it available via PMPs.

WE ARE ALL IN THIS TOGETHER

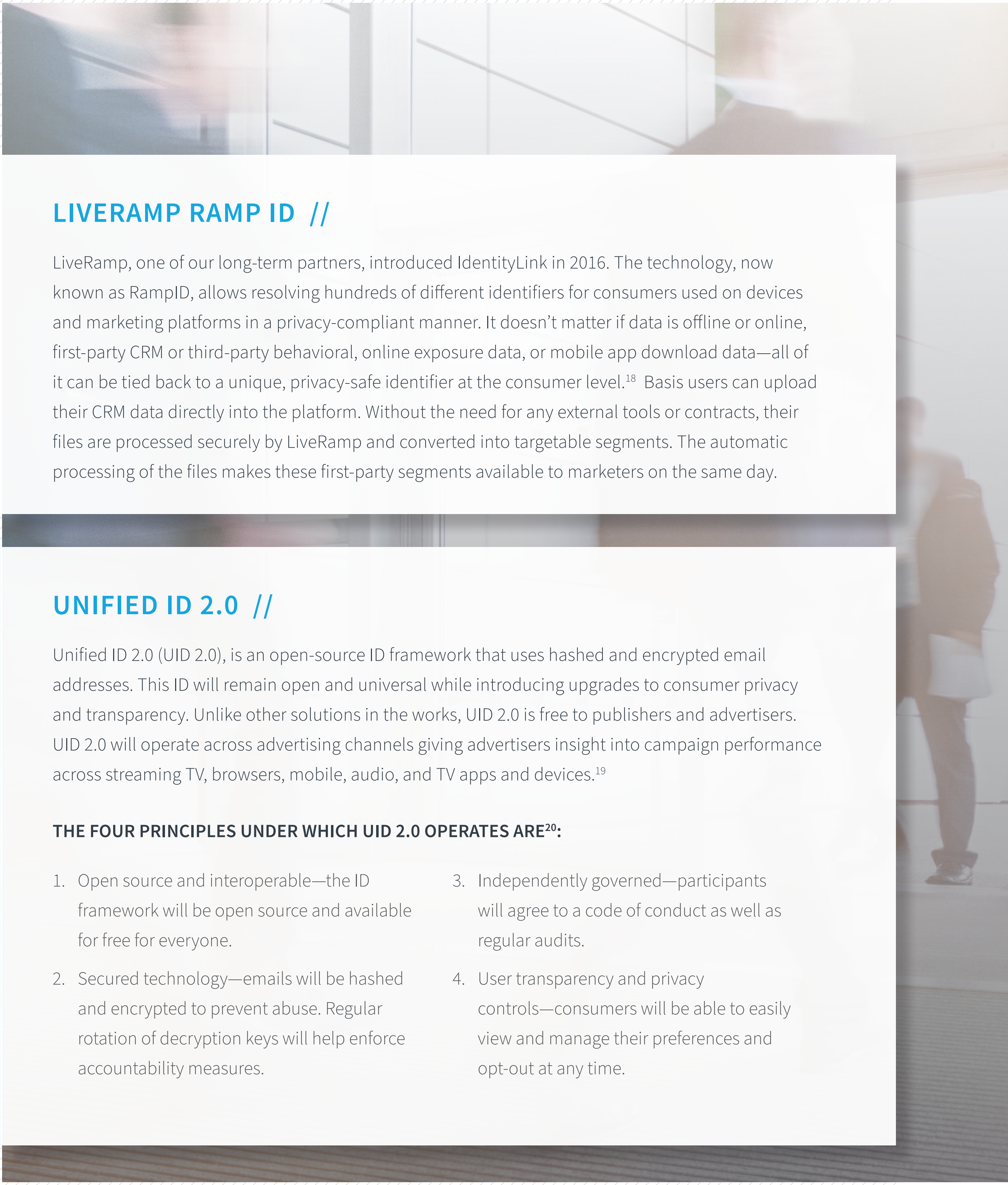
To prepare for a future without cookies, Basis Technologies has been closely watching and collaborating with other members of the industry. The success of an identity solution is heavily dependent on scale, and therefore partnering with an independent owner of a solution with the most scale, or partnering 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, IAB Project Rearc, and the open-source Unified ID 2.0 framework. We believe these identity solutions will not provide enough scale due to publisher-side adoption and are investigating multiple other solutions to adopt.

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, introduced IdentityLink in 2016. The technology, now known as RampID, 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.

UNIFIED ID 2.0 //

Unified ID 2.0 (UID 2.0), is an open-source ID framework that uses hashed and encrypted email addresses. This ID will remain open and universal while introducing upgrades to consumer privacy and transparency. Unlike other solutions in the works, UID 2.0 is free to publishers and advertisers. UID 2.0 will operate across advertising channels giving advertisers insight into campaign performance across streaming TV, browsers, mobile, audio, and TV apps and devices.[19]

THE FOUR PRINCIPLES UNDER WHICH UID 2.0 OPERATES ARE[20]:

1. Open source and interoperable—the ID framework will be open source and available for free for everyone.
2. Secured technology—emails will be hashed and encrypted to prevent abuse. Regular rotation of decryption keys will help enforce accountability measures.
3. Independently governed—participants will agree to a code of conduct as well as regular audits.
4. User transparency and privacy controls—consumers will be able to easily view and manage their preferences and opt-out at any time.

Conclusion

It's a new era for ad tech, 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.

THE WHAT, WHY & HOW //

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, 2022 - *https://gs.statcounter.com/browser-market-share/desktop/worldwide*

08 // Stat Counter, 2022 - *https://gs.statcounter.com/browser-market-share/desktop/united-states-of-america*

09 // Stat Counter, 2022 - *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/*

19 // The Trade Desk, 2020 - *https://www.thetradedesk.com/us/news-room/the-trade-desk-adds-nielsen-to-unified-id-2-0-initiative-as-advertisers-seek-upgrade-to-cookies*

20 // The Trade Desk, 2020 - *https://www.thetradedesk.com/us/news-room/the-trade-desk-adds-nielsen-to-unified-id-2-0-initiative-as-advertisers-seek-upgrade-to-cookies*

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