GOOGLE'S DECISION TO RETIRE THIRD-PARTY COOKIES

AN ACXIOM POINT OF VIEW

PURPOSE OF THE DOCUMENT

On Tuesday, January 14, 2020, Google announced that it intends to end support for third-party cookies in its Chrome browser. What follows is Acxiom's assessment of the situation and guidance related to Google's decision about third-party cookies, which are critical to much of the digital advertising ecosystem.

THE SITUATION

It is important to understand what Google announced—that third-party cookies will no longer be supported by the Chrome browser by the end of 2024. This is a similar action to what Apple took with its Safari browser in 2018. Google's Chrome and Apple's Safari own most browser traffic, so this does create a tipping point in the industry regarding how to acquire and manage data supplied by cookies. As the Interactive Advertising Bureau (IAB) stated in a post about its newly announced Project Rearc, this move by Google means the "default future state of digital media will be 100% anonymous, non-addressable to third-party vendors that support advertising-funded media and services today."

This will have the greatest impact on digital channels that rely on reach as a key benchmark for targeting audiences. Third-party cookies are what allows marketers to target in an anonymised state across digital channels. So, without them, we will see less advertising personalisation, decreased ability to retarget, reduced conversion insights and a need to increase focus on identified matching and reach in digital channels. This also makes onboarding offline data to online

> “Without third-party cookies, we are only left with per-domain identifiers using first-party cookies, and it becomes impossible for third parties to set or recognise any form of shared or universal ID across domains—for any purpose”, said Jordan Mitchell, the IAB Tech Lab’s Senior Vice President.

more challenging, as advertisers will now need improved identity management to scale audiences in a post-cookie world. Those impacted the most will be demand side platforms (DSPs) and platforms that depend on third-party cookie syncs to identify individuals across sites. So, without third-party cookies, we will be forced back to originating match and reach based on personally identifiable information (PII).

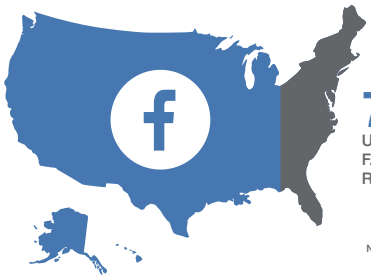
This is an industry-wide challenge. The MarTech and AdTech space is committed to increased consumer privacy without sacrificing commerce or access to content. We expect to see significant changes to support that commitment over the next few years. There will be an increased need for advertisers to develop more robust identity and data management solutions to achieve the marketing performance they were able to achieve prior to a cookie-less world. Acxiom is well poised to lead our clients through these confusing and changing times since we are experts at identity management and PII-based matching in privacy-conscious ways both online and offline.

WALLED GARDEN DUOPOLY IN THE NAME OF PRIVACY

Many will contend that a cookie-less ecosystem will increase consumer privacy and ensure digital privacy. While this is true, it will also strengthen the grip of the “walled gardens” on the digital advertising market. Two of the largest and most influential walled gardens are Google and Facebook. With their global reach, authenticated user traffic and closed advertising stacks they have an outsized advantage.

As mentioned, Google is in a dominant position in terms of internet traffic with 81% of the search engine market and 60% of browser penetration. Since the search engine is the gateway to the internet for a vast majority of users, this puts lots of power and influence in Google’s hands.

81%
OF US SEARCH ENGINE MARKET IS OWNED BY GOOGLE



70%
US ADULTS USE FACEBOOK ON REGULAR BASIS

NUMBER OF PEOPLE THAT FACEBOOK REPORTS CAN BE REACHED WITH ADVERTS ON FACEBOOK

2.121 BILLION

PERCENTAGE OF ADULTS AGED 13+ THAT CAN BE REACHED WITH ADVERTS ON FACEBOOK

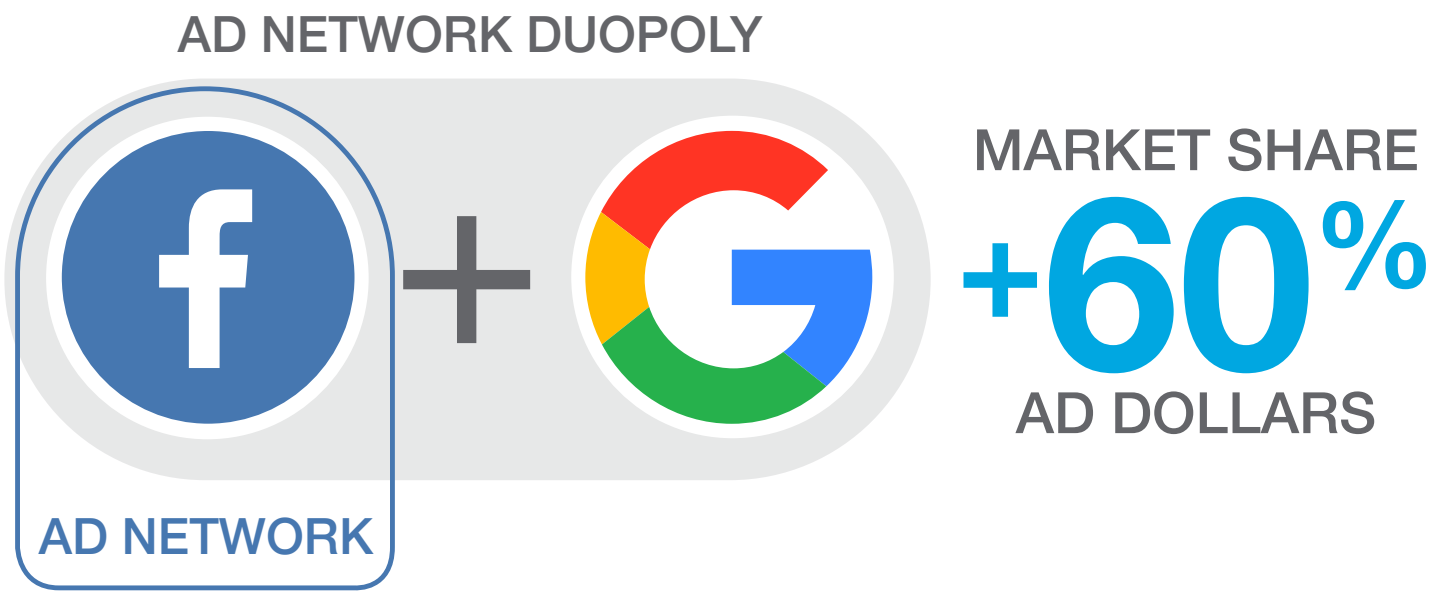
35%

Similarly, Facebook has a broad reach to more than 70% of U.S. adults, and more than 35% of the world's population. These statistics are evidence that the current ecosystem has created a "walled garden duopoly" between the two platforms.

The sheer reach and control of their platforms give the duopoly a huge advantage in reaching consumers and capturing their behaviours, intents and attention. This puts them in the lead position for capturing ad spend.

In a perfect world, brands would have complete transparency between both publishers. However, Google and Facebook can calculate and display ad performance statistics as they wish, with limited accountability.

Despite Google's stated intent to increase consumer privacy by eliminating internet behaviour tracking through cookies, the duopoly of Facebook and Google has a lot of economic interests at play. Google and Facebook don't depend on third-party cookies; however, the rest of the internet relies on the technology to track users across sites. Eliminating third-party cookies further solidifies Google's and Facebook's control of the ad spend market which was valued in excess of $129 billion in 2019, of which they already capture 60% (source: eMarketer, "U.S. Digital Ad Spending 2019").



BACKGROUND: FIRST- VS. THIRD-PARTY

	FIRST-PARTY COOKIES	THIRD-PARTY COOKIES
What's the Difference?	First-party cookies are set by or on behalf of the website the user is on. For example, if you are on Brand.com, first-party cookies are set by Brand.com. First-party cookies have traditionally been safe from automatic blocking or removal, as they are responsible for providing a convenient and seamless user experience. For example, first-party cookies are useful for storing: • User login status, which can be used to keep you logged in to websites and applications • Which products were added to shopping carts • Website settings, such as which language version was chosen • Favorite teams, sections, newsletters • Values entered in forms (e.g. name, email address, and company on a white paper download form)	Third-party cookies are set by domains other than the one being visited directly, hence the name. Third-party cookies are more frequently deleted by users, and more methods that block third-party cookie tracking are now being implemented. There are also increasing requirements for third-party cookies for privacy-centered regulations, such as the GDPR and CCPA. Third-party cookies are useful for: • Ad retargeting services (Double Click, Criteo, Adroll) • Programmatic ad buying • Cross-site tracking • Data sharing between third parties (cookie sync to share IDs and/or data) • Social share buttons • Customer service pop-up windows • Collecting website behavioural data for use in ad targeting • Measuring campaign performance by tracking which cookies were exposed to an online campaign
The Limitations	First-party cookies can only be read when a user is visiting the domain of the website/publisher. • Cross-site tracking is not possible • Advertising on other sites based on behaviour on the advertiser's own site is not possible • Retargeting is not possible	According to a recent report[1], 64% of cookies will be rejected. Rejection occurs when a browser either blocks a cookie from being placed at the time of the ad impression/site visit, or deletes the cookie after the fact. Data leakage is also a concern with third-party cookies. • Many third-party cookies get blocked, as browsers can mistake them for spam • Measurement relying on cookies is incomplete due to blocking and deleting • A cookie's information can be stolen if the session in unencrypted, so it's important to limit what is stored in them • There could be other tracking options and/or data that a third-party company is collecting and adding to the cookie that you are not aware of • Anti-spyware programs often delete this type of cookie
Solutions Enabled	Personalisation, preference management, shopping carts, customer personas, conversion tracking	Anonymous visitor recognition, programmatic ad buying, ad targeting, ad retargeting, behavioural ad targeting, behavioural analytics, measurement, behavioural data
Data Being Produced	Captures login data or web form data, behavioural data such as pages visited on the domain/website, browser/device setting information, time of use	Behavioural data across the internet, personal data (if readable), websites visited, time spent on websites

WHEN WILL THEY END?

2017

Apple's Safari crusade against cookies starts with Intelligent Tracking Prevention (ITP).

2019

From June 2019 FireFox blocks ALL third-party cookies and first-party cookies by default.

2020

Apple Safari blocks third-party cookies by default as of 2020.

2024

Google will begin ending support of third-party cookie tracking.

Google's Chrome browser will phase out third-party cookies by 2024, according to its recent announcement. Google Chrome is betting that its Privacy Sandbox—the privacy-preserving API unveiled in August—will build functionality that replaces third-party cookies. "We are confident … mechanisms like the Privacy Sandbox can sustain a healthy, ad-supported web in a way that will render third-party cookies obsolete," said Justin Schuh, Director of Chrome Engineering.

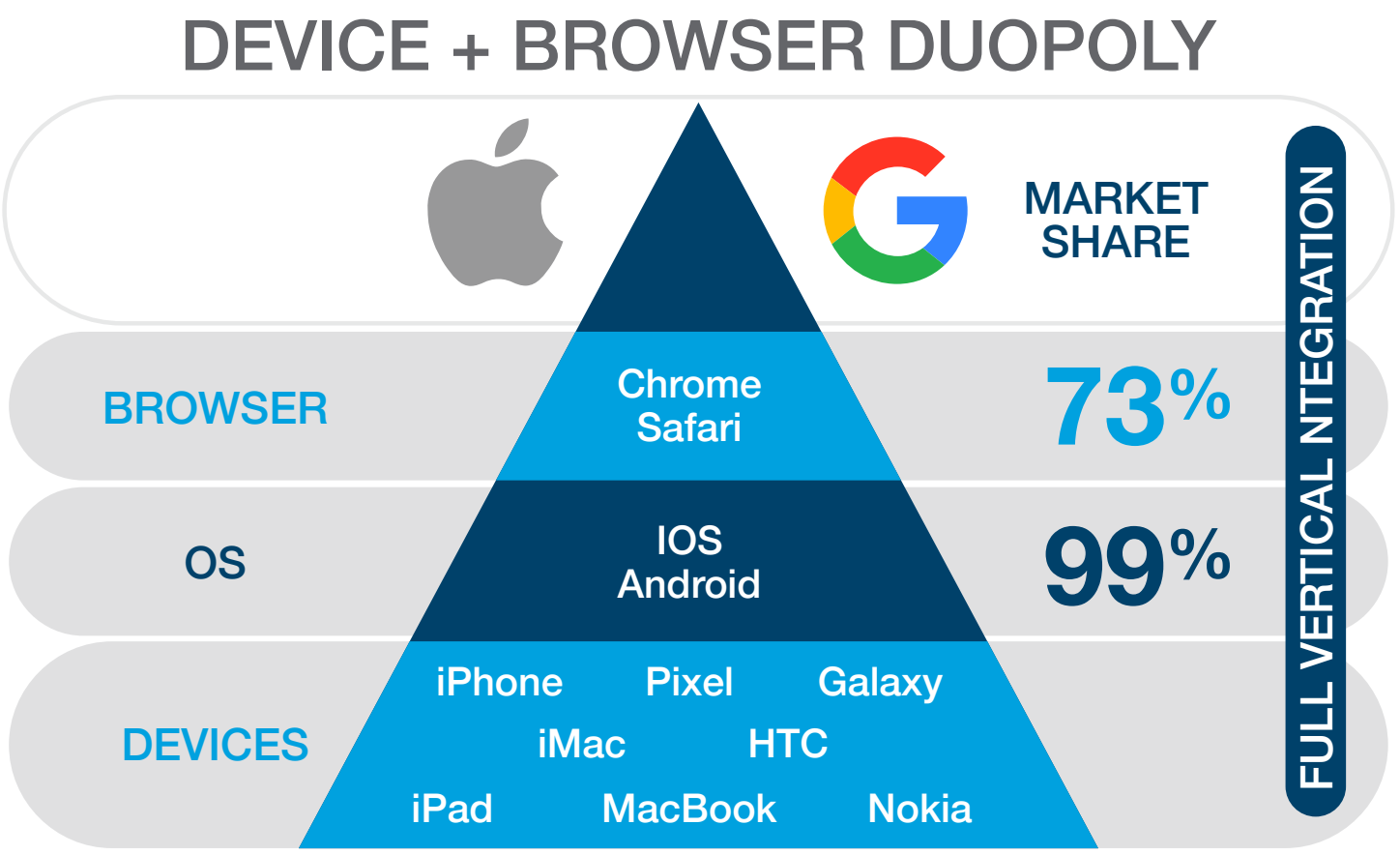
While this announcement was specific to Google, the implications are industry-wide. Google is not the first to kill third-party cookie access. Previous versions of Apple's ITP (1.0 and 1.1) allowed cookies to be read and used in a "third-party context," provided the user accessed the domain directly in the first 24 hours. That gave an unfair advantage to Facebook and Google, as the 24-hour purge didn't have the same effect on them as on other sites because users visit these websites regularly and rarely log out.

In Apple's newest version, ITP 2.0, the Safari browser detects cross-site tracking and partitions (or isolates) first-party cookies, making it impossible to use them in a third-party context for tracking or analytics. Some experts say that by introducing such strict rules to deal with third-party cookies, Apple sabotages the current economic model of the internet. With Google following suit, it is inevitable that either the economics of the ad-supported internet model are radically changing, or new and emerging solutions must come to the forefront.

WALLED GARDEN. CONTROL THE INTERNET. CONTROL EVERYTHING.

Google's dominance and control of the ad spend market is based on its full vertical integration across core platforms and systems. Google's services and products stretch all the way from consumer device manufacturing, to operating system and browser development as well as foundational AdTech capabilities like its own DSP, ad server and massive-scale content platforms. As noted by Keach Hagey and Rob Copeland of The Wall Street Journal, "Google's ad-tech business consists of software used to buy and sell ads on sites across the web. The company owns the dominant tool at every link in the complex chain between online publishers and advertisers, giving it unique power over the monetisation of digital content. Many publishers and advertising rivals have charged that it has tied these tools together—and to its owned-and-operated properties like search and YouTube—in anticompetitive ways." This integration allows Google to deploy its own "walled garden" that doesn't leverage third-party cookies.

Achieving scale and adoption across the stack is paramount to capturing ad spend and consumer influence. While Facebook doesn't have the browser, it has the most popular applications (e.g. Facebook, Instagram) on the internet and has the most organic reach of any platform.



THE IMPLICATIONS

THE PROS	
Added Protection to Consumer Privacy	Consumer privacy rights must be balanced against the need for ad optimisation, especially when there is no expressed consent given by the consumer. Such tracking is increasingly viewed as a violation and is specifically prohibited by privacy regulations. In an effort to overcome historical disregard for consumer privacy and consent, innovative technologies built with privacy-by-design principles will establish higher standards for personalisation and pseudonymisation. https://www.allaboutcookies.org/privacy-concerns/ https://www.adexchanger.com/data-driven-thinking/dmps-arent-dead-but-they-must-continue-to-evolve/
Removing Cumbersome Technology	Cookie syncs will be replaced with a single, consistent ID that will be leveraged by publishers, platforms and advertisers alike. This will inherently increase match rates across the AdTech ecosystem. This eliminates the cumbersome third-party cookie which was never an ideal solution for advertising and marketing purposes. https://medium.com/1plusx/the-death-of-3rd-party-cookies-what-google-chromes-tracking-protection-will-look-like-1e1817a42d0e
Standardisation Across Browsers	Google's announcement to eliminate its use of third-party cookies comes on the heels of similar moves by Safari and Mozilla. With Chrome owning 60% of browser-based traffic, this will certainly drive standardisation across all the major browsers and force everyone to work toward a better solution.

THE CONS	
The Unbalance of Power	Facebook and Google are selling their own inventory while also representing the demand side and controlling the price of their ad slots. With control of internet traffic there is very little the rest of the players in the AdTech/MarTech ecosystem can do but comply with Google's, Apple's and Facebook's rules. While 60% of internet screen time is spent on the open internet (brand sites), more than 90% of ad growth is owned by Google and Facebook.
Lack of Reciprocal Transparency	By forcing advertisers and publishers to embed Google and Facebook tracking pixels on their sites, they are further tightening their stranglehold on user data, gathering even more information by monitoring user activity on external websites. As the providers of the main tracking and reporting tool to monitor the performance of the campaigns on their networks, Google and Facebook can calculate and represent statistics as they wish, unchallenged.
Added Duopoly Exploitation	The behemoth companies that control internet traffic while also controlling browser and/or device-level controls are only positioned to further exploit this power "in the name of privacy." This is especially true for companies like Amazon that can learn from brands that utilise its platform yet won't provide consumer-level transparency back to the brand.
The Nefarious Hack	The more cookie-blocking tools are used, the more incentive websites will have to use other, less-transparent methods to infer identity without a cookie. These can be nefarious hacks that work similar to a cookie, or they can be probabalistic methods that attempt identification with some degree of confidence. Either way, this would swing the pendulum back in the direction of sites knowing a massive amount about their users without the users' awareness. This con is already being identified and discussed.
Access to Content	Free and open content on the web is critical to society. This content is almost entirely supported because of the money generated through advertising, much of which is dependent on third-party cookies.

THE IMPACT ON THE OPEN INTERNET

THE UNBALANCED IMPACT	
Independent Ad Exchanges	Many of the independent ad exchanges like Open x, Criteo, AdRoll and others depend on third-party cookies to follow a user across sites for retargeting display ads and to enable programmatic ad buying.
Commissioned Affiliates	There's an essential need to share information between brands and affiliates that request accurate, persistent, and deterministic cross-device tracking.
Third-Party Referential Device Graphs	Companies like LiveRamp, Neustar, Signal and others offer digitally focused identity resolution with heavy reliance on third-party cookies.
Multi-Touch Attribution	Depending on the direction Google, Apple and other walled gardens take, measurement across these walled gardens to achieve multi-touch attribution services from independent MarTech providers could become even more difficult. Walled gardens, such as Facebook, already prevent this.
Brands	Brands will need to update their tech stacks and strategic data partnerships to build and feature their own independent PII-based identity spines. In a post-cookie ecosystem brands must be able to share their independent graphs with their own sub-brands and media agencies to onboard to digital platforms. This is true for both the supply and demand sides whose channels are either non-cookie based from the start or have inventories with compliant signals that the brand's tech stack can connect to through strategic onboarding partnerships. This will continue to drive trends across the industry in establishing strategic partnerships while driving further market consolidation and innovation, thus rebooting the next phases of digital marketing. We will continue to see brands' media dollars drive the necessity for stronger strategic partnerships to reach their customers and prospects on the open web to justify their media spend. By establishing true transparent strategic partnerships, brands will continue to rely on their data partnerships to ethically enable and expand their customer base throughout the digital ecosystem as the industry adapts to overcome hurdles established by walled gardens.
Publishers	Publishers, especially less-known ones, depend heavily on advertising revenue to fund their content. The use of programmatic ad buying and ad exchanges gave publishers easy access to advertisers. Programmatic ad buying depends on third-party cookies. Alternative forms of making it easy for publishers and advertisers to connect will be critical to all but the largest publishers and for robust content on the web.
Consumers and Society	Content on the web is generally free and abundant because of the funding for advertising. (See Publishers section.) With a reduced ability to produce this content, the access to content will be reduced, which in turn threatens commerce and even a free and informed society.

THE POSSIBILITIES

Acxiom is well positioned to help agencies and brands manage the impending changes. We work with a wide swath of platforms and providers across the MarTech/AdTech ecosystem and have the necessary influence and connections. Whether integrating new technologies, leveraging platform relationships or working with industry-wide consortiums, we can tailor our solutions to meet the changing requirements. In addition, Acxiom has long been a privacy leader and advocate. We are following and participating in a growing number of possible innovations to support both the improved privacy and control by consumers while not unduly hindering commerce. Here are some of the active efforts and ideas:

1. Anonymisation and Psuedonymised Aggregated Microsegments

Privacy-Compliant Aggregated and Obfuscated User Segments

The 5th Cookie Initiative is a joint initiative of the IAF, Anonos and Acxiom. The term "5th Cookie" is a metaphor that encapsulates the goal of leveraging GDPR-compliant pseudonymisation to bridge "consent gaps" when consent by itself is no longer enough. "Demonstrable accountability" leveraging auditable and documented technical safeguards is necessary to balance data innovation and the assurance of the full range of individual rights.

- Under GDPR, compliant pseudonymisation requires that re-linking/re-identifying should not be possible without access to additional information kept separately and used only for authorised purposes (Article 4(5)). This enables the achievement of the principle known as "Aristotle's Golden Mean," which says that on a spectrum, an excess of behaviour sits at one end and a deficiency of behaviour sits at the other. But somewhere in the middle is a perfectly balanced behaviour: the golden mean. To achieve this balance, GDPR-compliant pseudonymisation bridges the "consent gaps" so both privacy and utility can be fully maximised.
- Under GDPR, encryption is state of the art for protecting data when at rest and in transit (Article 32). Similarly, pseudonymisation—as newly defined in GDPR—is state of the art for protecting data when in use (Article 25). GDPR-compliant technical and organisational safeguards in the form of digitally enforced pseudonymisation controls can be embedded in and flow with the data. This helps enforce risk-based data protection policies, which resolves conflicts between maximising data value and protecting fundamental personal rights to privacy.

Dr. Sachiko Scheuing, European Privacy Officer for Acxiom, said: "Augmenting the options of so-called walled gardens and contract-focused solutions with GDPR pseudonymisation-enabled micro-segmentation techniques is consistent with the principles embodied in Acxiom's "data ethics by design" framework. The 5th Cookie model could provide consumers with enhanced privacy while allowing effective marketing. Acxiom is committed to helping ensure data flows in the AdTech space in a way that complies with legislation and is used ethically, enabling data to be used to provide both maximum value for brands and privacy for consumers."

https://www.5thcookie.com/

2. Privacy Sandbox

Aggregated and Obfuscated User Segments

Google has proposed the implementation of an API call to a browser-based privacy sandbox which stores individual user-level information, but exposes personalisation and measurement data without violating user privacy. Similar to Google's ads data hub (ADH), this solution maintains privacy while supporting brands needs for targeted marketing. In 2024, Google will cut off access to DoubleClick IDs which are currently the only way to analyse user-level information in campaigns within ADH.

Google plans to begin trials for click-based conversion measurement without the use of third-party cookies. Since the conversions will be tracked within the browser, advertisers will be able to call an API that will send the conversion value from the browser. This allows AdTech providers a means to target aggregated cohorts, or groups, of site visitors without the granular targeting of specific individuals, thus maintaining privacy regulation compliance.

https://www.adexchanger.com/online-advertising/google-chrome-will-drop-third-party-cookies-in-2-years/

3. Cookie Replacement Technology

OEM-Driven Identification

Cookies are browser-based technology. One alternative is for key OEM providers to provide more organic and standardised identity solutions. Due to the limited number of OEM providers, it is feasible that an industry standard could be employed to create a consistent identifier. However, in many ways this puts the identity fabric into the hands of a few large providers and risks furthering a monopolistic culture.

The same is true for the browser developers. If Google, Apple, Microsoft and Mozilla were to standardise on a solution and create a ubiquitous browser ID then the need for third-party cookies would be circumvented. Unfortunately, this would only raise the walls on a few walled gardens, and put the open internet at risk.

PATH 1 – create a device ID applied to desktop or laptop computers; a browser on a phone or laptop would integrate with OEM manufacturer

PATH 2 – new browser ID, isolated to Chrome and not integrated with the phone or computer manufacturer

4. Consortiums and Collaboration

Authenticated Traffic Solution

LiveRamp's response to cookie-less tracking is the authenticated traffic solution (ATS), which leverages publisher first-party authenticated identity to provide addressability without third-party cookies.

ATS allows in-network publishers to match user authentication data, such as an email address, with LiveRamp's IdentityLink graph, which does not rely on third-party cookies. By matching on deterministic data, publishers can expand the addressability of their inventory in cookie-less environments.

The ATS integration with DSPs will connect user authentications with the corresponding LiveRamp IdentityLink, to the DSP publisher ID, giving publishers both a cookie-less identity solution and an immediate opportunity to leverage their data to increase yield and monetisation.

However, there are questions about what brands will do with non-authenticated site visitors, since that accounts for a large portion of visitors to sites that aren't behind a pay wall or even a free-access wall.
Long-tail publishers and small and medium businesses will be at a disadvantage since the friction resulting from authentication requirements will further erode their number of visitors.

"The people with signed-in users are going to win," said Megan Pagliuca, Chief Media and Data Officer at Hearts & Science. In this case, grounding the identifier on first-party data will create "more of a disadvantage for the mid-tier and long-tail publishers that don't have [a sizeable number of registered users]," Pagliuca said. (Source: Digiday) "The industry is looking to first-party data to replace cookies, but the open web may lose out."

https://www.prnewswire.com/news-releases/liveramp-taps-openx-as-authenticated-traffic-solution-ats-exchange-partner-300957583.html

5. Private Exchange and Ad Network based tracking

It takes a village.

Epsilon-Conversant believes an "exchange-based solution" is the answer. With an inventory of more than 2,000 advertisers and publishers, it utilises what it calls "header bidding" via a server-side API. By collecting privacy-compliant user information across a large client base, it is able to deliver relevant ads to in-network visitors while maintaining the proper level of anonymity.

Similarly, it is important to note the recent announcement of Merkury, "an identifier designed to allow marketers to continue targeting audiences online without using third-party cookies" (source AdExchanger, "Merkle Launches An Identity Solution As The Industry Weans Off Cookies" by Alison Weissbrot).

"Consumer privacy and the death of the third-party cookie are changing the rules for digital and cross-channel marketing," said John Lee, President of Merkury. "Going forward, both marketers and publishers will begin with their first-party relationships to create owned, private identity graphs that generate addressability while maintaining their own intellectual property. These brands will be able to network their private graphs with partners and publishers to increase addressability for all in a privacy-conscious way. Merkury's mission is to serve as a neutral technology enabler of the private graph, supporting seamless interoperability between brands, publishers, and technology platforms."

While this is a legitimate solution if achievable at scale, there are plenty of challenges to this model as there are already a growing number of competing exchanges and architectures.

6. First-Party Authentication

Focusing on Contextual Marketing vs. Behavioural

Some activists and organisations are pushing for a complete elimination of cross-device and cross-site personalisation for non-authenticated users. This is the most conservative approach as it would only allow brands to retarget site visitors who make themselves "known" on one of their owned websites. Brands would move back to focusing on contextual marketing and reduce models and strategies relating to behavioural analytics.

7. Consumer-controlled, Consent-based Identifiers

Establishing technical standards for companies' first-party solutions

The Interactive Advertising Bureau ("IAB") Tech Lab, in its Project Rearc proposal, introduced a plan to develop rigorous technical standards and guidelines that inform how companies collect and use a consumer-provided, consented identifier tied to privacy preferences. Consumers would be in control of the use of the ID and any related data. Businesses would strictly adhere to any privacy preferences attached to the identifier and the identifier would be sufficiently encrypted so that it couldn't be reverse-engineered to identify the person. Any third-party vendor tracking would only be done with explicit consumer consent, and only on behalf of the trusted first parties. The IAB, however, is not providing a specific identifier product or service like others have launched, but rather providing technical standards for companies to apply to their own first-party solutions.

8. Brand Gardens

If you can't beat them, join them.

Following the footsteps of Google, Facebook and Amazon, the last possibility we will include is the concept of brands building their own walled gardens. This is only feasible for a handful of global brands that have the number of site visitors and the content necessary to keep and maintain a first-party cookie pool of significant scale. However, it is feasible that a few big brand walled gardens could build their own site network and monetise their authenticated traffic.

KEY TAKEAWAYS

1. We have a short amount of time to figure this out. This impacts the entire ecosystem, and everyone has a vested interest in architecting the next generation of advertising-supported free internet.
2. First-party data and first-party site authentication will continue to rise in value.
3. People-based third-party data assets like those managed by Acxiom are not affected and will continue to be valuable in segmenting and onboarding audiences for programmatic distribution.
4. Expect a significant increase in publishers requesting payment for content and cross-publisher consortia as businesses look to monetise their content as advertising revenue declines. This will invariably have a negative impact on the long-tail publishers and small to medium businesses.
5. New privacy and risk management technology will become a popular way to securely match first-party PII between parties without data leaving its original location.
6. Google and Facebook are not trying to end an ad-supported internet, so they will be offering alternatives that will give brands a way to buy and sell advertising inventory, although it may be focused on their individual walled gardens.
7. Consumers will be given more precise controls over privacy while still being served with relevant advertisements.

[1]Flashtalking Quarterly Cookie Rejection Report, March 2018, https://www.flashtalking.com/cookie-rejection-report.

acxiom.co.uk • ukenquiries@acxiom.com

ACXIOM