WHAT'S NEW IN PUBLISHING

INSIGHT REPORT

HOW PUBLISHERS CAN SWAP OUT THE COOKIE JAR IN 2021

Written by:
Hazel Broadley

Sponsored by:
sovrn

FROM OUR SPONSOR

Identity resolution is one of the biggest challenges facing publishers. Once the third-party cookie goes away, publishers and advertisers will no longer be able to rely on a single, easily accessible and shareable ID.

THE FUTURE OF ADDRESSABILITY

But the balance of power is shifting. Advertisers will soon become more dependent on publishers to provide them with the audiences and data they need. We're committed to supporting all of the solutions that will give our publishers the ability to succeed in this new environment, from supporting universal identifiers to providing answers to your unauthenticated traffic. Remember—the more information you can provide, the more you stand to benefit.

In sum: identity is opportunity.

Yours,

sovrn

Power to the publisher.

Contents

How publishers can swap out the cookie jar in 2021

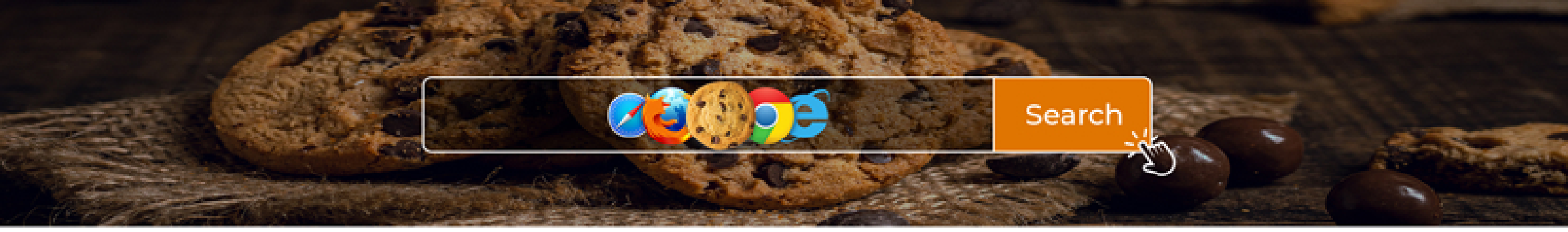
Introduction – state of the industry

A great deal has been written about the deprecation of the cookie since the first major players began switching off third-party cookies. Fast forward to 2021, and the developments seem to be moving at a much faster pace – this time with Google firmly in the spotlight.

First, the tech giant announced it would switch off third-party cookies within two years. Soon after, the Competition and Markets Authority (CMA) launched an investigation into the company's suspected breaches of competition law. Then came two further announcements from Google: firstly, that FLoC (Federated Learning of Cohorts) would replace third-party cookies; and secondly, that it would cease to collect advertising identifiers in iOS.

With key stakeholders confirming that the majority of digital advertising still relies on third-party cookies, now is the time for publishers and brand advertisers to consider how they might best survive the soon-to-be depleted cookie jar. However, as the IAB's latest update reveals, there is a distinct disconnect between the importance of post-cookie-era solutions and business readiness. In fact, two-fifths of respondents (40%) admit they aren't fully prepared for the change.

In this report, we take a closer look at the current advertising ecosystem, as well as examining how the industry is responding to the cookie challenge. We also ask industry leaders their opinion on the steps publishers can take, as well as which emerging solutions, or combination of solutions, might help publishers pave the way forward in this cookieless future.



How reliant are publishers on third-party cookies?

The simple answer is that it's hard to measure accurately, with a wide range of estimates across the industry. At the conservative end of the scale, Chris Hogg, EMEA Managing Director at Data Management Platform (DMP) Lotame, says *"from our data, around 50% of the web is on Chrome, where third-party cookies are still available"*.

Remi Cackel, Chief Data Officer at global media platform Teads, reports that *"most digital ad spend relies on cookie-based data. Third-party DSPs are bidding on average 75% less when a third-party cookie is not available."* With far-reaching impacts across the entire marketing cycle for brand clients, these impacts *"are kept hidden today as cookies are still largely usable for around 65% of global web traffic"*. For publishers, meanwhile, the challenge will focus on inventory monetization capabilities, which is *"directly based on the diminution of the eligible demand observed on the client side. Publishers also need to be proactive about the cookieless situation to future-proof their business and revenues"*.

Cory Munchbach, Chief Operating Officer at pure-play Customer Data Platform (CDP) BlueConic, states that *"anything programmatic is essentially third party. In fact, nearly 85% of the top 1,000 sites have cookies set by a third party, which highlights its prevalence"*.

Meanwhile, Mattia Fosci, Founder and CEO at EU-funded privacy-first DMP, ID Ward, expects third-party data to be present in *"99% of ad transactions"*.

Why are major platforms switching off third-party cookies?

Before we answer this question, it's important to note that although some browsers are no longer supporting third-party cookies, they haven't been blocked altogether. Whereas cookies in Chrome are currently turned on by default, by 2022 they will be turned *off*. Inevitably, this does mean that a large proportion of audiences will likely become invisible overnight. So, why the shift?

USER PRIVACY

Over the years, DMPs have developed increasingly sophisticated technology – including AI – to harvest inordinate volumes of data, segment it, and sell it onto third parties. Unlike first-party data (directly from customers and prospects), and second-party data (obtained from a data partner in a strictly one-to-one permission-driven environment), the origins of third-party data are much harder to track. What's more, even though cookies don't include PII (Personally Identifiable Information), they can still allow an individual to be tracked by their location via mobile ads.

USER EXPERIENCE

Harvesting details in this way not only compromises user data but also detracts from the user experience. In fact, it has driven over a third of consumers (36%) in Europe to turn to ad blockers to prevent being spammed with irrelevant or repetitive advertising – rising to 67% of Chrome users. In addition, the sheer volume of third-party trackers in use – surpassing a thousand in some cases – is causing unacceptably high levels of latency.

36%

of Europeans have turned on ad blockers to prevent spam and advertising

A SECONDARY BENEFIT FOR MONOPOLISTS?

Ironically, as a consequence of turning off cookies, many smaller publishers and brands who advertise on these large tech platforms will find it harder to gain full visibility into their campaigns and maintain a direct connection with their customers without huge investment. Commenting on the potential for tech platforms to leverage this opportunity, Cackel says *"third-party cookies are based on a 90s sub-optimal technology which creates unneeded complexity (in terms of both privacy and the unsustainability of the millions of cookie-matching requests which take place every second). While the latest Google proposal would surely solve those two points, these changes should not be a pretext for competitive advantage (e.g. removing granular targeting capabilities for the publishers and only allowing it within walled gardens and social platforms)".* Given Google's vested interest (nearly 90% of its revenue depends on tracked advertising), the consensus is that it will hold true on its assurances of developing robust and ad-friendly replacement technology well before switching off cookies.

What alternatives will Google provide?

FLoC:
Perhaps the most important initiative revealed is FLoC, which groups users based on similar interests while keeping individuals anonymous. Google reports that testing has been promising, with nearly a 350% improvement in recall and 70% in precision. However, as VideoWeek observes, FLoC is not a “wholesale replacement for third-party cookies”. While the API enables targeting based on users’ interests, it does not solve issues such as measurement and fraud prevention.

Trust Tokens
Another initiative in progress is to replace the cookies with Trust Tokens, which authenticate a particular user (while remaining non-personalized and cryptographically-signed), before placing users in aggregated groups.

TURTLEDOVE
Meanwhile, TURTLEDOVE, which stands for “Two Uncorrelated Requests, Then Locally-Executed Decision On Victory”, works in two stages. First, a contextual ad request and an interest group ad request are sent at different times. This de-correlation prevents enriching any type of contextual ad request with interest group information, and vice versa. Second, the ad auction occurs client-side rather than server-side, so that the platform conducting the auction cannot tie the two requests together. Google is also currently testing an expansion on this proposal known as FLEDGE.

Looking towards a cookieless future

Living in a post-cookie world may seem daunting for publishers, but the advice from tech providers is unanimous: **by looking into alternatives in good time and working collaboratively where appropriate, publishers can help brands get even closer to their audiences. By being prepared, remaining transparent and fostering a culture of trust and loyalty, everyone stands to benefit.**

To help prepare for the changes, in December 2020, a dozen UK publishers consulted with the IAB's Tech Lab to explore the "expected impact on ad targeting and real-time bidding within the open marketplace". It goes without saying that privacy will also be key. As Matt White, Vice President EMEA at Quantcast sums up: "Whatever the publisher landscape that emerges after third-party cookies, the successful solutions will be the ones that put consumer privacy first".

Meanwhile, Hogg says that Safari and Firefox *"only ever really had 20%-40% of the browser market share, so there's always been enough inventory, whether it's by using apps, or the Safari and Android identifiers, or whether it's just through the main browser, which has been Chrome for a long time. By using new technology such as Lotame, Chrome users can now be added into the pool. Larger publishers may be able to use a walled garden approach, using their own ecosystem of registered users and contextual targeting. However, they are unlikely to compete effectively against [the largest players], with their sheer volume of registrations and email addresses, because they control both the authenticated accounts and the ad ecosystem. Moving data from an open industry standard (third-party cookies) encourages heavier reliance on proprietary systems".*

So, what solutions are available?

Fingerprinting – more harm than good?

Browser (or device) fingerprinting is a method used to cross-track users between websites without using cookies or IDs. Instead, website code is used to test the presence of certain attributes to identify a device. The ‘fingerprint’ is the combination of probabilistic attributes (rather than deterministic cookies attached to a browser), which can then be used to track the user.

Fingerprinting is categorized in four ways: browser parameters (browser name and version, screen resolution, IP address, location); demographic attributes (age, gender, occupation) obtained from supposedly anonymized consumer data traded for marketing purposes; browsing history (although Apple, Google, and Mozilla have since taken steps to mitigate this); and canvas fingerprinting (instructing the web browser to “draw” a hidden image that can be turned into a unique ID).

Despite its use on a quarter of the top 10,000 websites, the accuracy of fingerprint matching is thought to decay quickly over time, from 98% (compared with deterministic matching) within 10 minutes of the attribution; 80% between 10 minutes and three hours; and 50% between three and 24 hours. Indicating that **fingerprinting is not a viable (nor moral) method for publishers**, there is a distinct correlation between the decline in fingerprinting and the rise of persistent identity solutions.

Identity solutions – the ideal scenario?

There are two types of identity solutions. **'Authenticated web' solutions** attach data to a persistent, unique ID, such as an email address and login to enable **deterministic matching**. Authenticated IDs currently available include GAID (Google Advertising ID), Apple's IDFA (Identifier For Advertisers), The Trade Desk's Unified ID 2.0 (open source, rather than proprietary), ID5 (an independent solution), and the Advertising ID Consortium's ID (an independent group of ad tech companies using LiveRamp's IdentityLink).

In contrast, '**unauthenticated**' or '**open web**' **solutions** use signals and algorithms (increasingly using ML) to identify the same user across different devices and apps (known as **probabilistic matching**). Device clusters (e.g. the devices a person might use with the same IP address, location and websites visited) can help build pretty robust probabilistic data. Although less accurate than deterministic, it does have the ability to scale. As Hogg estimates, *"the open web will account for around 70% of all inventory, because, as a user, you don't ever log into every website you use each day. For instance, you might wade through five different food sites before finding the perfect recipe to download"*.

Highlighting the importance of identity, Zara Erismann, MD Publisher Europe at LiveRamp, explains that *"publishers and marketers who haven't yet started their post-cookie journey need to focus on addressability. It is too important to be ignored and there is merit in acting with urgency. Addressability – through people-based identity – provides a direct link to audiences. Without it, a publisher's ability to target, measure and provide detailed attribution for marketing efforts will be reduced significantly"*.

Meanwhile, Quantcast is ramping up its deterministic offering by expanding its existing Consent Management Platform (CMP) to provide user permissions across multiple sites. Permisio is free to all existing publishers and focuses on the user. Early adopters can create an account and set their privacy preferences for each site, or a general profile across all sites. The benefits are 1) publishers have consent to collect first-party data about the user to inform targeted ads, and 2) users see fewer permission pop-ups and have a central portal to control their data. As White explains, *"consented first-party data from sources like Permisio combined with ML capabilities will provide publishers with access to great audience insights long into the future"*. The challenge, however, will be gaining enough exposure, and therefore uptake, to make a meaningful impact in the industry.

Data enrichment solutions, such as Lotame's Panorama ID, could be the most effective way to attain scalable quantities of privacy-compliant, pseudonymized data in the years to come, with each individual ID *"carrying an average of 200+ behavioral attributes"*. Because users' data will be stored on different IDs, Hogg advises publishers to ***"look at using DMPs which overlay multiple data sources to enrich inventory"***. Panorama ID is a *"probabilistic solution that helps publishers collect identifiers and put them into cohorts"*, so you may have three or four or five devices that connect together with first-party cookies coming into the mix.

Meanwhile, InfoSum offers an interesting approach to identity resolution with its privacy-by-design technology that "keeps datasets isolated, encrypted and anonymised". Rather than the information "being moved into one pot, a decentralised network builds virtual bridges between datasets".

The number of identity solutions on the market certainly suggest this is where the future of publishing is headed.

Should publishers focus on deterministic or probabilistic data

The two properties of third-party cookies which made them so useful – accurate tracking and ubiquity – have been separated, hence the need for new identity solutions to fill the gap. But should these focus on deterministic or probabilistic data?

Deterministic data – which should also be authenticated data – is more likely to be compliant with privacy regulations and is more accurate. Probabilistic data is still a legal grey area. As a recent Winterberry Group report suggests, almost any user data can fall under GDPR due to *"the flexible definition of personal data, where almost any attribute can be considered personal data if it may be combined with personal details at a later stage"*.

On the other hand, probabilistic data can have a far wider reach, as it doesn't rely on users being logged in to every website they visit. As Hogg mentions, by adding in probabilistic data, *"publishers will pick up incremental inventory and eyeballs just from people browsing through the internet"*. It's also really important to bear in mind that **fresh probabilistic data can be better than stale deterministic data**. Knowing with 70% accuracy that a user is car shopping today is more useful to an advertiser than knowing with 100% accuracy they were fridge shopping two weeks ago. As White agrees, *"third-party data can be useful in some instances if vetted carefully; the dangers lie in stale, poorly labelled data"*.

Ultimately, it's a trade-off between a safe bet (relevancy and compliance) for a small audience versus a weighted throw of the dice on a large audience. Some solutions are attempting to circumvent the issues with probabilistic tracking by combining many different sources of first-party data, which brings us to data collaboration.

Collaborative solutions (and clean rooms) come to the rescue

It seems the ability to 'go it alone' is increasingly unrealistic, with the exception of a small number of scalable walled gardens. As Hogg highlights, *"even your first-party data has a shelf life, so potentially, you can't use the data you collected the day before. Also, when a user logs onto their devices in the morning, they could show as having 30 different user IDs, in part due to browser erosion, where browsers are not only blocking third-party cookies, but forcing the deletion of first-party cookies on a regular cadence. Meanwhile, all third-party data was first-party somewhere along the line"*. Therefore, it's **not necessarily true that all first-party data is good and all third-party data is bad. It seems the overriding factor is how it's been treated**.

Munchbach agrees: *"I don't think all third-party data needs to be considered bad, but there are too many unanswered questions out there right now. Is the data consented? What is the lineage? How old is it? I think a better approach is to start with first-party data and then judiciously assess whether third-party data is necessary, based on these questions. With a pure-play CDP, there's very little reason to use third-party datasets"*.

One issue for Fosci is that *"merging information creates new information. Has the user consented to merging that data with other data so that new things can be learned about them? The GDPR is very clear; it says you need to ask consent for the specific use of the data [at every stage of the journey]. Relying on first-party data means 60-70% revenue losses for publishers. And that's taken from Safari, which has already banned cookies. This is where data collaboration comes in"*.

So, which different collaborative solutions can publishers leverage?

1. Data cooperatives, originating in the 90s using offline data, allow multiple brands to provide first-party data for combining. Examples include The Abacus Alliance (Epsilon Abacus), The Alliant DataHub (Alliant), Datalogix (Oracle), Apogee (Data Axle) and Donorbase (Lake Group Media).

2. Data marketplaces and data exchanges allow third-party data to be exchanged for targeting or analysis. Publishers can search data sets and select best audiences for activation (e.g. Adobe's Audience Marketplace, Eyeota, LiveRamp Data Marketplace, Lotame, Oracle DMP, The Trade Desk, Tru Optik and Snowflake).

3. Data clean rooms (or technical data environments), originally designed as a way of matching offline data to a brand's CRM, now offer publishers a compliant, accurate way of comparing their brand advertiser data against walled garden internal identity graphs, to prevent over-serving ads to the same audiences. The data never leaves the clean room, so publishers don't actually need to give up their data (but share it in a way that protects each party's proprietary assets). Typically, the larger walled gardens don't share with each other, so advertisers still run the risk of duplication and therefore over-investment in these platforms. However, Unilever is developing a clean room in partnership with Google, Facebook, and Twitter, where advertisers should be able to see duplicated reach on these platforms. Currently, 42.9% of US brand marketers and 30.3% of UK brand marketers are leveraging clean rooms such as those offered by Lotame, Acxiom, or InfoSum.

With data sharing capabilities predicted to increase from 2021-2024, through a *"near continuous process of testing, similar to the early days of programmatic between 2009 and 2012"*, **collaborative solutions such as clean rooms are definitely worth considering, especially for larger publishers**.

However, Fosci does offer a word of caution: *"Often, matching data doesn't work or isn't very accurate. The industry average is about 40% [match rate]; there's a big chunk of IDs that simply don't sync well. Therefore, there are a lot of company acquisitions motivated by access to first-party data"*. So, with a risk of collaborative solutions being hampered by privacy legislation, is there a way of using the data without breaking compliance? Arguably, edge computing provides a perfect solution.

Enter: edge computing (the era of zero-party data?)

A relatively new technology, edge computing collects and analyzes behavioral data on the user's device to serve them targeted ads (rather than sending the data to be processed on a server as with most behavioral targeting). The advantage is that it minimizes the data leaving the user's device, protecting their privacy and remaining compliant, while also preserving personalized ad space. **Edge computing also circumvents restrictions on the amount of data allowed to be sent into the bid stream**, either through legislation (e.g. GDPR) or browser technology (e.g. ITP).

Edge computing is unique as it doesn't use IDs but rather an abstract description of the user identified across segments (e.g. 'baking' and 'dessert recipes'). When an ad request or bid request is made, the abstract description is shared with the SSP or DSP respectively. **Although ad tech is a nascent use case for edge computing (time will tell if it delivers on the promise of speed, accuracy, and impact on CPMs), it does seem to offer the optimum balance of user privacy and publisher insight**.

Claiming a 100% match rate, Permutive has established itself as a leader in edge solutions for many publishers including Dennis, Business Insider, Condé Nast, Immediate Media, and The Economist. As David Reischer, Head of Product at Permutive, explains: *"user data, by design, is protected because it never leaves the device. This means a publisher can process their first-party data in a world without cookies and with increased government regulation – even under its strictest interpretations. Permutive uses data about authenticated users (~10% of visitors) to extrapolate and produce a predictive model about the unauthenticated visitors (~90%)."* Using Permutive, publishers can collect for instance 20 or 30 customized real-time data points, or 'events', about visitor behavior in a single anonymous pageview (e.g. article title, author or category).

Meanwhile, ID Ward is a privacy-by-design initiative partially funded by the EU, not only due to its alignment with the EU's privacy and sovereignty agendas,

but also its vision of protecting the diversity and financial sustainability among (smaller) European publishers. Pushing the boundaries of innovation in edge computing, ID Ward's solution goes one step further by not limiting publishers to domain data. The platform uses ML to offer publishers insights about their audience cohorts (user churn rate, apps used etc.) and complements Google Analytics, measuring traffic to and from a publisher's website. But, at the same time, it uses edge computing to keep the data anonymous.

As Fosci explains: *"We manage the whole data lifecycle from collection to the creation of the anonymous audience segments. And in all that, we are not preventing publishers from also viewing and exploring their own data with their own tools. But we can give publishers the benefit of targeted advertising with full compliance; we also can give them anonymized information about their audiences, which they can use for subscriptions.* ***The engine that's powering personalized, targeted advertising is the data that sits on the device, so it's zero-party data in that respect"***.

A potential drawback is that to achieve a swing of market power, publishers would need to 'fill in the gap' by modelling and segmenting users. This would require substantial investment, perhaps negating any server cost savings. In addition, to be scalable across different publishers requires agreement on a common taxonomy for the abstract description of the user. Also, the valuable nanoseconds saved by removing the need for ID matching might be negated by the solution demanding more of a user's hardware resource – on a device currently less powerful at data processing than a DMP or CDP – potentially resulting in latency. In contrast, as Pranay Prabhat, Senior Director of Digital Ad Technology at NYT suggests, *"server-side processing is especially important to keep our front-end web and mobile apps lighter and faster"*.

However, as device technology evolves in general, edge computing will definitely become a more scalable solution. Interestingly, alongside Permutive's and ID Ward's DMP solutions, a new privacy-first browser has also emerged, from Brave. Its Brave Ads program uses granular profiles controlled and maintained by the user and incentivizes users by offering 70% of the revenue shares in BAT (Basic Attention Token), a reward point redeemable within its loyalty platform.

Beware of behavioral, count on contextual

With around 86% of programmatic ads in Europe using behavioral data, conventional wisdom is that behavioral targeting improves campaign effectiveness, and therefore, advertisers pay more for behavioral data. However, there is little empirical data showing that behavioral targeting alone significantly improves publishers' revenues. A recent study assessing the impact of cross-tracking ads on publishers found only a 4% gain in revenue ($0.00008 per ad). With the financial and reputational cost of compliance potentially outweighing any small gain in revenue, contextual may be a better bet.

Before the advent of the web, behavioral advertising didn't exist; all targeted advertising (TV, print) was contextual. Combined with programmatic trading, contextual ushered in the dream of one-to-one advertising and is still a viable method of monetization today. Contextual relevance can make ads more engaging and memorable, and can also prove more effective than behavioral for a geographically local campaign in terms of Cost per Acquisition (CPA). As per the earlier car vs fridge scenario, contextual ads can be more engaging, as they more closely match the user's real-time intent, rather than perceived intent based on how they behaved two weeks ago.

Looking beyond a sole reliance on first-party data, Reischer says: *"By embracing the anonymous web, publishers can also reach the audiences they want in a contextual, relevant, and timely way. It will mean moving from a world of one-to-one marketing to one where audiences, not individuals, are key". Meanwhile, Cackel explains: "Contextual targeting doesn't require the use of cookies and is definitely not a plan B. Teads has been using it across industry verticals and markets, and successfully provides similar media effectiveness to clients. Contextual targeting works harder with quality content, and this should be a key focus for publishers to thrive and differentiate themselves".*

Modern-day contextual targeting – which has evolved into ‘contextual intelligence’ – uses AI and ML to achieve:

- **more accurate and granular categorization of content**
- **more dynamic content at the page and post level (e.g. ‘www.bbc.com/news’ could be ‘News’ at the top level, but ‘www.bbc.com/news/technology’ could be ‘News’ and ‘Technology’)**
- **capabilities across more languages**
- **sentiment analysis and mitigation of mismatched ad placements to improve brand safety for advertisers. For example, previously a recipe website might have excluded the words “hash” and “herb” to avoid association with content related to illegal drugs, thereby making it difficult to reference “hash browns” and “herb-cheese omelets”. Sophisticated contextual solutions also go beyond text to recognize images, video, and audio.**

British startup Illuma Technology has developed proprietary AI to improve contextual targeting by reading live contextual signals that are driving interest and awareness of brands on the web. The platform then uses these to expand its search and identify new prospects for relevant ads in real-time, which it then serves programmatically. As a recent Kantar study reveals, Illuma’s technology grew ad awareness by almost 12% (65% above Kantar’s UK norm), and brand affinity (“an important yet difficult metric to shift”) by almost 15 percentage points.

Following a period of heavy focus on behavioral targeting, it seems an AI/ML-supercharged contextual comeback is presenting a major advertising opportunity to fill the void. Other contextual intelligence solutions and initiatives include Beemray, The Ozone Project, and Comscore.

Bridging the gap

In what's turning out to be an exciting era for the online ad industry, we're seeing the emergence of a new technology known as 'moment targeting'.

As Peter Mason, Co-founder of Illuma, explains, moment targeting fuses behavioral targeting with contextual, with AI forming a bridge between the two. It uses real-time audience insights to prospect contextually, reaching people when they are most receptive. ***"Advertisers benefit from the scale and anonymity of contextual while maintaining the relevance of behavioral targeting. Moment targeting delivers results across a range of KPIs, from brand-based metrics such as reach, video views and brand uplift, right through to performance targets such as form fills and sales"***.

Importantly, this type of targeting is unaffected by browser changes and doesn't use personal data. Instead, campaign moments are defined using live page data, making moment targeting a compliant and future-proof option for marketers in the privacy-first world.

Supplementing with subscriptions

The consensus among industry leaders is that regardless of other solutions being adopted by publishers, renewing focus on building a first-party subscription base is crucial. As Mason advises: *"publishers – particularly small to mid-tier – should think about growing their first-party audiences and learning as much about them as possible. Simple steps might include gating online content with passwords and driving newsletter subscriptions"*.

Success stories include The Spectator, which more than doubled conversions in three months and is forecast to reach 100,000 subscribers in 2021. The publisher achieved this by streamlining the entire subscription process (from login to payment to checkout) with the help of Piano, an e-commerce optimization and analytics solution providing out-of-the-box templates and segments that allow the creation of customer journeys at speed.

The advice from industry leaders is to offer a value exchange and make users feel like an exclusive member of a club. To tailor content to subscribers (or prospective subscribers), it should be localized, personalized, publisher-specific in terms of perspective, relevant to daily life, delivered at a regular cadence, and optimized to provide the best user experience.

As Erismann stresses, *"while it is part of building a longer-term strategy, publishers need to be looking in-depth now at how they develop authenticated audiences, for example by an individual registering on a website, signing up for a newsletter or accessing a community forum with their email address. At the core of this process, publishers need to look at the value exchange they are entering into with the customer, which means offering meaningful content, experiences and more"*.

Whereas publishers used to believe that readers wouldn't pay for content, most publishers (78%) charge for digital access, with the majority (80%) offering a limited number of articles, and over half (57%) limiting access to five articles or fewer per month. Therefore, publishers should consider using a metered model rather a hard paywall. However, as Hogg warns, *"walled gardens may not be viable for small and medium-sized publishers [that rely more heavily on pass-through traffic]. Publishers that do have strong subscriptions are leaning towards mixtures of identity and context". White adds: "Not all publishers have the brand recognition necessary to command subscriptions, and a barrage of logins will diminish the browsing experience. This is why Quantcast focused on developing Permisio"*. Other vendors offering subscriber analytics for publishers include Chartbeat, Oracle NetSuite, and SimilarWeb.

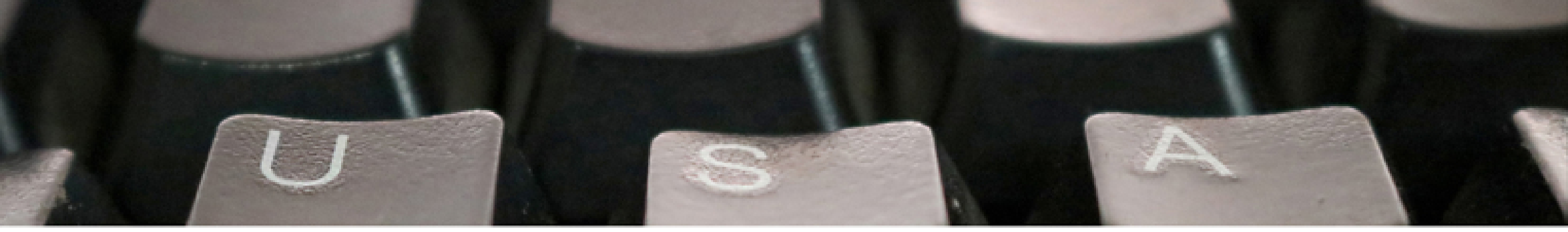
Vertical ad networks (niche networks for niche titles?)

In the late noughties, vertical ad networks became popular among publishers as a privacy-friendly way of dealing in ad inventory for specific topics to target an audience based on their interests (technology, automotive, travel), as opposed to a horizontal ad network dealing with a wide variety of inventory. Tapping into a vertical ad network is a privacy-friendly way of targeting, as you're focussing on the content rather than the user. However, it's only viable if your content falls into one of a few specific niches; otherwise, you may see CPAs increase as the ads become less relevant. Nowadays, most networks seem to have been replaced by other technologies, or been built on top of horizontal ad tech, although some still exist today, such as GourmetAds (food and wine) and its subsidiary HealthyAds (health, fitness, and medical).

Key takeaways: so, what's next for publishers?

Act now, hone later
As we bear witness to a number of solutions emerging on the market, it's important to at least consider – if not act upon – these strategies now. As Cackel suggests, they *"have to be initiated now to be fully ready for 2022 when cookies disappear. Some of the required changes, e.g. introducing a login in the user experience of their website, has to be anticipated. Iterations and A/B tests will be required to find the best approach. The future is now".* *White adds: "The faster publishers can build their own first-party data, the better placed they'll be to thrive into the future. Those who have a direct relationship with their audience will be able to monetize their traffic more easily. For publishers who don't have the established brands to sustain subscription models, the challenge will be acquiring this data without putting all their content behind logins which will impact the browsing experience.* ***Luckily, companies like us are working to roll out products which put consumer privacy first while enabling publishers to build ad-funded business models – and for small and mid-tier publishers, there are free tools available in-market already that allow publishers to collect consent on a more sustainable, cookieless basis, to make sure the open internet can thrive"***.

Test and test again
As Hogg reminds us, publishers should "test solutions and strategies while third-party cookies are still around to compare against. Ask for PoCs around Safari and Firefox inventory. The fact that we don't have cookies in some of the other browsers presents a good opportunity for publishers to test out solutions and tactics today rather than later". Erismann adds: "There needs to be a focus on developing and/or fine-tuning strategies for driving authentications. Creating successful authentication strategies means optimizing the various tools publishers and brands have at their disposal, such as subscriptions and newsletters, social logins, premium subscriptions or offerings, content walls, and gated or premium services. These then need to be tested and iterated until they resonate effectively with the target audience".



Dare to diversify

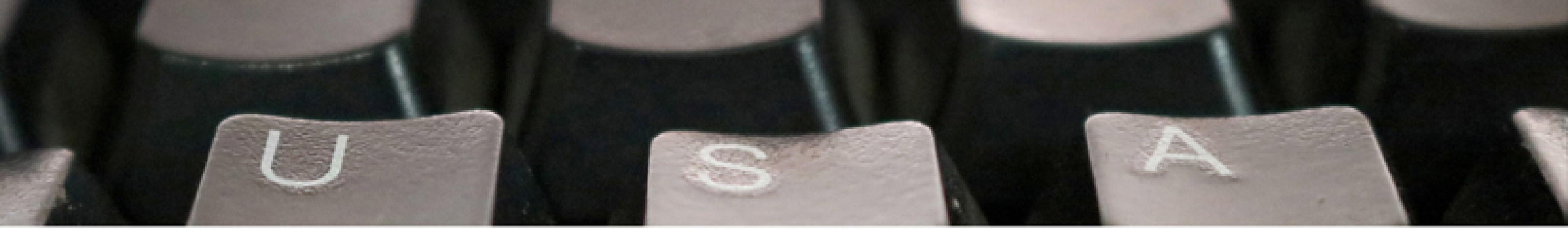
For Fosci, the key is diversification. *"Being small doesn't mean that you don't provide value; it just means your audience is smaller. If you're a niche publisher with a loyal audience, try to create a subscription model or a freemium model. While it may not be viable to hire a full-time data analyst, don't underestimate the importance of analysis on your bottom line. Publishers should have more control of their audience data, but do not need to build their own in-house solutions. History shows that these investments rarely pay off as the technology evolves too fast. Instead, publishers should work with partners that protect and enhance their relationship with their own audiences".*

Remain agile

Munchbach says that *"from a short-term perspective, publishers need to embrace agility so they can switch up their strategy as the situation dictates. We saw this with Covid, when publishers removed their paywalls in a matter of hours in an effort to get information out to people. When there's a huge breaking news event, publishers need to be empowered to make changes in the moment to capitalize on the opportunity".*

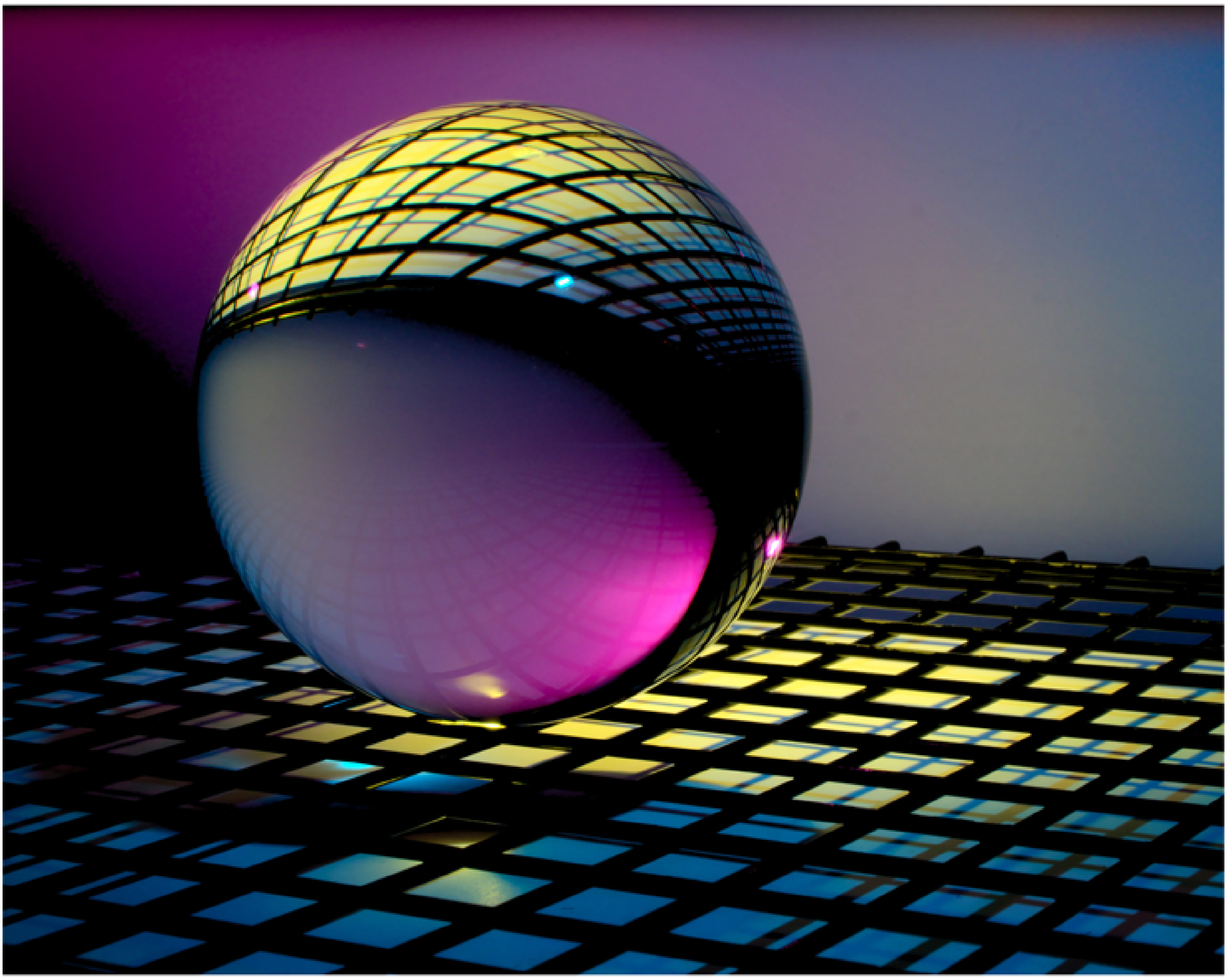
The future lies in contextual intelligence, clean rooms and edge computing

While replacement of the cookie with a single universal technology will take time, in the short term we are likely to see a fracturing of ad tech, with several competing replacement technologies appearing before we can determine which will emerge dominant in the marketplace. As Reischer believes, *"publishers should have a louder voice in these conversations, especially premium publishers with less dependency on open programmatic demand. At the moment proposals are very much optimized towards advertiser use cases, but we miss the voice of publishers protecting their interests, opportunities and data assets. The death of the cookie is a huge opportunity for publishers to course correct on what has happened, with their data being aggregated at scale, repacked and sold as audiences or models."*



In summary, publishers should avoid a sole reliance on fingerprinting, behavioral targeting, or vertical ad networks. Instead, they should focus on first-party subscriptions and innovations in contextual targeting – think moment targeting – while larger publishers should also consider collaborative clean rooms for accuracy, value and control. Finally, publishers should consider a data-conservative approach to selling remaining inventory via edge computing platforms.

Regardless of which solutions are adopted in the post-cookie era, through collaboration, confidence in their content, and creating a value exchange, publishers large and small can forget about the cookie jar and come out even stronger as we head into 2022.



ABOUT THE AUTHOR

Hazel Broadley

Having combined her love of linguistics with a career in tech marketing and PR, Hazel Broadley has spent the last decade compiling thought leadership content and reports on behalf of numerous ad tech companies. The founder of UK-based tech content writing consultancy, Lexical Llama, Hazel's specialty is delving into the latest industry issues and exploring disruptive technology.

ABOUT US

Founded in 2008, What's New In Publishing provides a single destination for independent publishing businesses looking for news, advice and education across a wide range of publishing subjects.

We cover developments in digital publishing, magazines, and newspapers, focusing on the issues and technological advances confronting the industry at a time of profound disruption, offering practical and useful advice from "What's New?" to "What Next?".

With many thousands of publishers worldwide subscribing to our weekly e-newsletter and many more visiting the site regularly, *WNIP* is one of the world's longest running and leading B2B websites covering the publishing industry.

whatsnewinpublishing.com

@wnip

WNIP
WHAT'S NEW IN
PUBLISHING