



WHICH WAY NOW? PUBLISHER OPTIONS FOR THE ENDING OF THIRD-PARTY COOKIES

Written by:
Hazel Broadley

Sponsored by:
SOVRN

Identity Solutions

Our approach to the identity challenge

Assign every visitor an identifier. Sovrn supports all identifiers.

Create and append segments to the identifier. Sovrn can help you enrich your user data.

Monetize with partners. Sovrn can help you activate your first-party ids and segments in the bidstream.

SOVRN CAN HELP:



Know Your Audience

Get insights into visitor behavior and engagement.

Use Sovrn's lightweight //Signal beacon to get insights like dwell time, scroll depth, engaged time and more.



Enrich Your Data

Scale your authenticated traffic and enhance your visitor profiles.

Leverage Sovrn's //Data Collective to enrich the data you already have by linking off-site behavioral or commercial data to hashed-emails.



Monetize Your Segments

Activate your segments in the bidstream using your first party data.

Using Sovrn's private marketplace (PMP), Prebid or your own ad server, ensure you maximize the value of your audience by monetizing your segments.

Contact us today to learn how Sovrn Identity Solutions can help you generate the greatest outcome from your visitors

sales@sovrn.com



Contents

Which way now? Publisher options for the ending of third-party cookies

- 4** Introduction: Google's latest reprieve is not a time for complacency
- 6** Big tech developments
 - FLoC takes flack
 - CafeMedia's FLoC Origin Trials
 - Apple's walled garden
- 12** Advances in ad tech
 - Developments in first-party IDs
 - Changes to contextual
 - Evolving edge computing
- 18** Next steps for publishers

Introduction: Google's latest reprieve is not a time for complacency




In January 2021, Google's cookie announcement prompted us to explore the implications for the publishing industry, which we presented in our report, [How publishers can swap out the cookie jar in 2021](#). But it also spurred a number of developments within the industry, and before we completed the report, the landscape was changing before our eyes.

As a result of these developments, publishers have been scrambling to adapt their strategy, and in some cases, their entire business model, in preparation for a world without third-party cookies.

In another dramatic turn of events, Google recently took the decision to [delay cookie deprecation](#) from early 2022 to late 2023. On the face of it, this extended period is needed for Google to implement [commitments](#) to its proposed privacy sandbox replacement, following the [antitrust investigation](#) by the UK's CMA (Competition and Markets Authority).

But one underlying reason is that publishers simply aren't ready with alternatives. In a recent survey, ENGINE Media Exchange (EMX) found that while [98%](#) of publishers plan to implement cookieless solutions, less than half have taken steps to do so. Google itself says, *"it's become clear that more time is needed across the ecosystem to get this right."*



Meanwhile, a [Teads](#) survey of over 400 publishers and media companies across 52 countries reveals that [more than half](#) admit they are unclear as to how cookieless solutions will impact their business. In fact, only a quarter (24%) say they have a strong understanding of all the new initiatives and their benefits and drawbacks.

As Teads' Chief Supply Officer, Eric Shih, sums up, there is a *“lack of clarity that publishers are facing when it comes to the death of the cookie. Despite being the ones most likely to suffer from impacted revenue streams, they're relying on spontaneous, and often confusing, updates from tech giants ... A set of future-facing targeting solutions is an essential part of that ecosystem.”* He believes there should be *“a concerted effort of collaboration and consistency from all parties involved to ensure ... privacy demands are respected, whilst still allowing free access to some of the best content on the open web.”*

But while it might be true that publishers need more time, this is not a time to become complacent and put off the search for alternatives. So, what is their best bet?

In our last report, we looked at a number of cookie replacements, such as identity solutions, collaborative solutions (and clean rooms), edge computing, behavioral targeting, contextual targeting, and subscriptions.

In this follow-up report, we revisit some of the most significant industry developments, including the two elephants in the room – Google's privacy sandbox and Apple's walled garden.

We then look at the platform solutions which appear to have advanced most significantly during this period of transition: identity solutions, contextual targeting, and edge computing.

Finally, we ask industry experts whether their advice for publishers has changed during this time, and how proactive they should be in light of the delay.



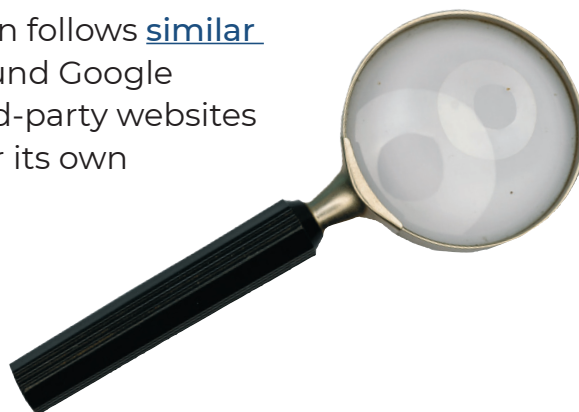
Big tech developments

FLoC takes flack

Although Google claims its privacy sandbox solution, [FLoC \(Federated Learning of Cohorts\)](#), will produce **95%** of the per-dollar conversions that third-party cookies previously achieved, so far it has met with widespread resistance. Although a number of companies are either testing the sandbox this year ([AdThrive](#), [CafeMedia](#)), or working with Google on their proposals ([PubMatic](#)), the criticism is certainly gathering momentum. This is significant, as ostensibly, Google is designing FLoC to become a fundamental part of the web, not just Chrome.

Several web browsers (Firefox, Brave, Vivaldi, and Opera) announced they [would not support FLoC](#) in its current form because it fails to provide sufficient user privacy. Apple's WebKit Security and Privacy Engineer John Wilander, perhaps unsurprisingly, expressed skepticism about the proposal. Meanwhile, privacy-minded search engine and direct competitor of Google, DuckDuckGo, [rejected it](#) outright. The initial CMA (Competition and Markets Authority) [investigation](#) to assess whether FLoC is likely to distort competition was followed by [a consultation](#) in June 2021 about accepting Google's commitments.

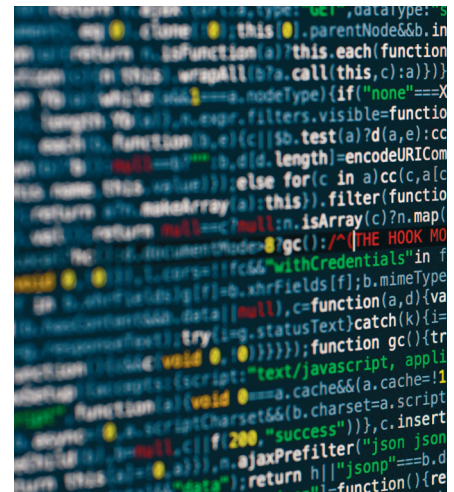
Scrutiny is perhaps prudent, since the European Commission also launched [its own investigation](#) into Google in the same month, this time to determine whether the company violated antitrust rules by favoring its own ads in the online auctions it manages using current cookie technology. Google had already been fined [€220 million](#) (\$268 million) in France for abuse of market power. The Commission's investigation follows [similar lawsuits](#) in the US, with concerns around Google restricting access to user data for third-party websites and apps, while reserving this data for its own gain.





Future PLC, a UK-based media company with a portfolio of over 50 brands, is backing the scrutiny as a chance to improve privacy compliance. Future's Global Commercial Operations Director, Nick Flood, says that with the CMA's announcement comes *"an opportunity for the entire ecosystem – including Google, advertisers, publishers and the ICO – to work together to meet privacy goals, and better serve the needs of consumers and advertisers alike. The conversations and actions already in progress as a result of Google's sandbox changes have rightly brought consumer privacy to the fore, and reflect a positive shift towards prioritizing audience needs."*

As far as tech vendors are concerned, aside from privacy, FLoC has other drawbacks which will likely result in it constituting only a small part of the replacement of third-party cookies. The consensus is that long-tail publishers alone (for example, recipe websites that some users only visit occasionally) do not provide enough valuable data for advertisers. A third-party tracer (e.g., cookie) benefits these publishers because it follows users around each website, providing more data to the long-tail site and improving the value of its ad inventory. FLoC is a continuation of this principle.



However, larger and more premium publishers are disincentivized from opting in because their sites provide a disproportionate amount of user data compared with smaller publishers. For instance, behavioral data from the *Wall Street Journal* will power impressions biddable on the recipe website. Furthermore, FLoC will require user consent, which will dramatically reduce its reach, especially in the case that Chrome is the only browser to adopt it.

For these reasons, Jakob Bak, Co-founder at **Adform**, believes large and premium publishers will experiment with FLoC, but that it won't constitute more than 30% of any media plan, and that ultimately, they will end up disabling it. *"In a data-siloed world, where larger publishers build data on top of their first-party IDs, long-tail publishers will lose out."* However, Bak believes this is a fairer ecosystem, since value is apportioned according to the data a publisher provides.



Alasdair Cross, VP Sales EMEA at cross-device ID resolution platform, [Rog.ad](#), agrees: *“the problem is that it’s effectively unattributable as they describe it, unless you set the interest category as a unique ID, which, inevitably, everyone will do, and the interest category will just act like a first-party cookie that only some DSPs have access to. Why don’t we skip to the end game and just use first-party cookies?”*

Meanwhile, the Teads survey reflects these sentiments, revealing that the following proportions of publishers are considering the [various alternatives](#) to third-party cookies: 27.6% are exploring first-party data, 27% contextual, 21.8% universal ID, and only 18% FLoC. So, if FLoC cannot replace third-party cookies alone, what will the rest of a publisher’s portfolio look like?

CafeMedia’s FLoC Origin Trials

Among the participants in the FLoC Origin Trials – in which a small number of Chrome users running a beta version of the browser have been assigned to FLoCs – is [CafeMedia](#). Although it is not yet being used by advertisers to target and buy ads, the trials do show how FLoC groups online users based on content consumption across 3,000+ sites that work with the publisher network.

FLoC works by using an algorithm to convert browsing history into a hash (a very long value), preventing the entire browsing history from being reconstructed. This is not revealed because it might only correspond to a small number of users and show information about their history. Algorithm values that are similar will have similar browsing histories. These are grouped and share a shorter version of the value. These groups are the cohorts, and their shortened algorithms are their FLoC IDs. A user can only be in one cohort at a time, although their cohort may alter if their browsing behavior changes. There are currently approximately 34,000 cohorts, but not every one will be seen. The system won’t use a cohort if it is likely to visit domains tagged as sensitive, or contains fewer members than the minimum (for privacy).

The fact that the similarity of the algorithm values correlates with the similarity of content means FLoCs with IDs closer to each other will represent more similar groups of consumers. For example, the highest value in cohort 17,000 will be similar to the lowest in cohort 17,001. However, there will be a degree of overlap between non-adjacent cohorts because content relationships are [not linear](#).

CafeMedia combined FLoCs into larger groups called ‘kFLoCs’, each containing 1,000 cohorts. For each kFLoC, CafeMedia has surfaced 10 content keywords that [over-indexed](#) compared with the average in that kFLoC. For example, kFLoCs 14,000-15,000 showed a pronounced index value for the key phrase ‘finance & technology’, so a brokerage firm searching for likely investors may look to test advertising in those FLoCs first.



Apple's walled garden

Apple's developments in user privacy, combined with the prevalence of its devices (there are now over [1 billion](#) active iPhones), are having a substantial impact on the ad tech landscape. Apple's [App Tracking Transparency](#) (ATT) went live with iOS 14.5 on 26 April 2021, requiring users' explicit permission to track their behavior across other apps and websites, with a prompt for each app.

ATT appears to be having a negative impact on behavioral ad revenue. A recent Consumer Acquisition report found that only [20%](#) of users are consenting to tracking, and that iOS advertisers are experiencing a 15-20% drop in revenue coinciding with increased unattributed organic traffic. The report corroborates an early Flurry Analytics [study](#), which found that the US daily opt-in rate was 12-14% (rising to 22-31% worldwide). This leaves a huge volume of users invisible to behavioral targeting.

Facebook's iOS advertising revenue is also reportedly [in decline](#) due to the low ATT opt-in rate. Brian Bowman, CEO and Founder of Consumer Acquisition, attributes the loss to a reduced ability to recognize look-alike audiences and users with the highest propensity to purchase (known as [value optimization](#) in Facebook Ads). *"There's a collapse of value optimization bidding. The ability to specifically target people who are going to transact is diminished, and will continue to erode as ATT rolls out."*

If users decline cross-app tracking, attribution falls to Apple's SKAdNetwork framework, which provides only limited information. Apple has made slight improvements, however, with the release of its [SKAdNetwork 3.0](#) in iOS 14.6 in May 2021. The framework now allows devices to send postbacks to multiple ad networks, including the winning networks and up to five losing networks. However, this may not [provide enough data](#), as it is not clear which five networks are chosen, and furthermore, they don't know why their attribution was lost.





Ingrid Couasnon, EVP EMEA, [Smart](#), says that “today, [SKAdNetwork’s] scope is too limited to be used at scale as it only enables conversion measures for app install campaigns.”

Cross agrees, saying that “in both SKAdNetwork and FLoC, attribution and retargeting become impossible. Multi-touch attribution becomes a distant fantasy. But the bright side is that publishers can turn to an alternative solution provider to fill in the blind spots.”

There have been subversive attempts to bypass ATT using probabilistic matching, including a [consortium](#) backed by the Chinese government, which dared Apple to ban all apps involved in one fell swoop. Apple has responded by [blocking any apps](#) using the system, known as CAID (China Advertising ID), and has prevented any app updates containing the ID from reaching the App Store.

The tech giant also announced [two new measures](#), at WWDC21, to counteract fingerprinting: ‘Private Relay’, which uses two relay systems to obfuscate a user’s IP address to hide their browsing information in Safari (like a VPN); and ‘Mail Privacy Protection’, which hides the user’s IP address so that senders are unable to connect the address to online activity, and are unable to see whether an Apple Mail user has opened the email. These measures will [likely restrict](#) ID graphs and targeting on CTV, which is heavily IP-based.



Some advertisers expect Private Relay, in particular, to be the [beginning of the end](#) for fingerprinting on iOS, as Apple starts a battle to stamp out the practice. Shumel Lais, CEO of mobile advertising analytics platform, Appsumer, views the feature as “a precursor to Apple using welcome technical solutions to break fingerprinting.”

While Apple has restricted behavioral targeting, it has also expanded its [own ad business](#), adding a new ad slot, ‘Suggested’, in the App Store. [Some reports](#) believe this expansion could be aided by their privacy moves. This has also elicited antitrust lawsuits in [both France and Germany](#).



However, Bak doesn't believe Apple is making a power play on the industry to build up its own ad business; instead, these developments are consistent with Apple's history and guiding principle of putting the consumer first.

While both Apple's approach and its ad tools have [drawn criticism](#), publishers cannot afford to exclude Apple's ads from their portfolio. As Mattia Fosci, Founder and CEO at EU-funded privacy-first DMP, [ID Ward](#), says, *"it would be silly not to embrace Apple ads, but it would be suicidal to only focus on Apple ads. Publishers need to keep their options open."*

In summary, behavioral targeting may become decreasingly effective on Apple devices to the point where it ceases to be worthwhile. If so, where does this leave publishers' ad revenue? Having concluded in our [previous report](#) that a portfolio approach is needed, let's explore which solutions are gaining traction in the industry.



Advances in ad tech

Developments in first-party IDs

For those publishers who have a more structured plan in place, first-party IDs certainly show promise. As the Teads survey highlights, nearly half of publishers are considering first-party data and universal IDs (28% and 22% respectively). Of those, nearly half (47%) will opt for logins compatible with either LiveRamp's IdentityLink or The Trade Desk's Unified ID 2.0. Although this already demonstrates an industry preference, the remaining 53% is still fragmented across other ID solutions.



Even though the cookieless future might seem a long way off, industry progress has been slow. For publishers still relying on third-party cookies, two years is a short space of time to transform their entire ad revenue model. So now is the time to put plans into action.

As Adform's latest [study](#) concludes, despite three-quarters of companies globally (75%) acknowledging that the deprecation of the cookie will impact their business, over three-quarters of marketers (78%) have no tested solution in place – and only 3 in 10 (29%) globally have adopted a first-party ID solution. In Europe, however, publisher adoption of first-party IDs is nearing third-party cookie volumes.

Adform says the introduction of its ID solution is already generating significant results. In fact, the [percentage](#) of publishers passing first-party IDs in the bidstream (according to Adform's largest domains that represent 80% of total ad spend with the company) is 100% in Denmark, followed closely by 93% in the UK, 90% in Spain, and remaining well above 60% in other European countries. In the US, it's a different story, with the number below 20%.

While over two-thirds of large publishers (68%) are passing first-party IDs, these are mostly on smaller proportions of their traffic (primarily authenticated users), bringing the overall volume down.

European traffic comprises predominantly random IDs and first-party cookies, whereas most US traffic comes from authenticated IDs such as LiveRamp or BritePool.

While authenticated IDs can carry more data, they don't scale as well as first-party cookies – Bak estimates that only 5% of the internet happens behind logins – and so they don't provide functionality such as frequency capping, profiling, reporting, etc. However, publishers seem hesitant to use logins in any case, with the Teads survey highlighting that almost two-thirds (65%) are not planning to increase their use of logins to specifically deal with third-party cookie deprecation, due to potential disruption of user experience, and impact on traffic.

Bak continues, *“We expect first-party IDs to overtake third-party cookies this year ... while publishers have proved they are ready, we now need the buy-side to ramp up adoption, and we're calling on CMOs to lead the charge. With the impressive scale now made available by publishers, it is time for brands to start benefiting on Safari and Mozilla while gaining important learnings on how to use first-party publisher IDs instead of third-party data. This is not a straightforward substitution that can wait until the last minute.”*



Customer Data Platform, [BlueConic](#) – which has just launched a [tool](#) to assess organizational readiness for a future of first-party data – also recommends that publishers focus on their first-party data above other ID solutions. BlueConic's COO, Cory Munchbach, says that many publishers are overwhelmed; stuck in a situation that is *“becoming more confusing thanks to the multitude of vendors proposing alternative solutions that supposedly address the fallout from the demise of the third-party cookie”*. Munchbach also warns that many of these solutions *“are merely third-party cookies in another ID's clothing. To future-proof revenue and customer trust, companies need to take back control of their data and build closer connections with their customers using first-party assets.”*

However, a single publisher's first-party data is not normally enough to replace the functionality of cookie tracking (unless the dataset is very large). Marketers want to know how audiences react to other brands. For example, although they may be confident that a consumer who makes a purchase from a particular brand is likely to be interested in other products by that brand, a missing element could be that the consumer enjoys home improvement, so is open to seeing other DIY-based products. Therefore, data on how a user interacts with a brand is a valuable part of predicting their purchase patterns.



With DMPs enriching first-party data and augmenting ad performance, the next step is for publishers, especially larger enterprises, to use their first-party IDs to collect data and profile users, making these available on DMPs.

Meanwhile, [The Ozone Project](#), owned and operated by a cohort of UK news publishers, has built an advertising and audience platform to provide an editorially-governed, GDPR-compliant “safe haven” for premium websites.

The platform claims to offer turnkey access to ad partners, while boosting ad partner match-rate, providing log-level transparency (showing winning and losing bids), and scaling pricing according to the volume of ad requests. Comscore data from December 2020 shows Ozone's network reached over [99%](#) of adults that month, boasting 2.5m unique visitors more than Amazon, 1.8m more than Facebook, and 66,000 more than Google.

Ozone's CTO, Scott Switzer, says that the platform “uses a combination of first-party data, a cross-device map, and verified data to create an identity graph across publishers. This graph will continue to function when third-party data is blocked by default in Chrome. Furthermore, Ozone has a transparent attribution framework where publishers are compensated for the data they provide to our audience graph.”

ID resolution platforms, which read and match different IDs to build an identity graph, such as Roq.ad's, are rapidly gaining a foothold in the industry this year. As a cross-device solution, Roq.ad believes their platform is more tenable than trying to force ID consolidation on the industry.

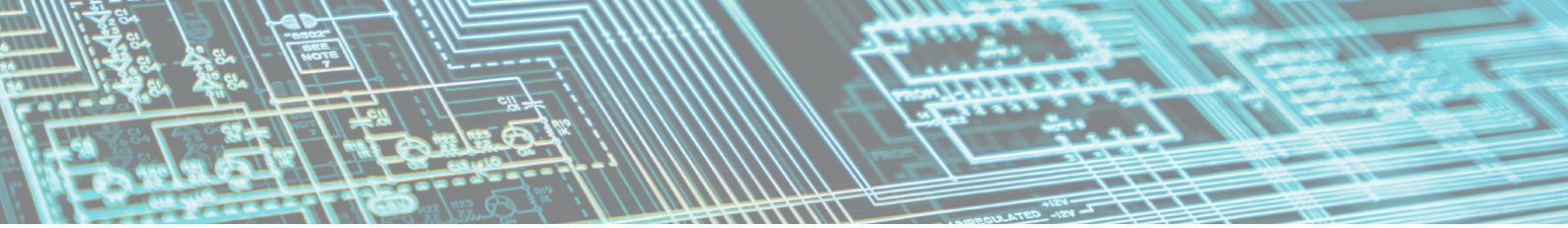
As Cross explains, “A number of identity resolution services are pushing the entire ecosystem to operate in their ID space, and have been doing so for several years. The Trade Desk, LiveRamp, ID5 and others have all recently played with open identifiers being “given” to the publisher community and other players in ad tech, but these are not new themes. One only has to go back as far as 2018 to know how identifier consolidation turned out for the folks using the [AppNexus ID](#) in its 2017-2018 incarnation. With the loss of third-party cookies entirely, the industry has an opportunity to not make the same mistakes again. If we all operate in every first-party cookie space simultaneously, we don’t need to have the same identifier. We just need a way to read each other’s respective identifiers.”

Cross continues, “instead of forcing the industry to adopt our language, we give our customers the tools to operate in their own language and get the benefit of understanding everyone else’s at the same time. I think this is the way forward for our industry. We are not in the business of hoarding personal data and spying on our users. We are in the business of learning about their interests and serving ads that might match them for our partners while respecting privacy all the way.”



Of course, data partnerships give marketers valuable data from which they can form insights about consumer behavior patterns. But privacy and security are key: data outside a publisher’s ecosystem must be truly anonymized. This can be done by methods such as tokenization, where information such as an account number can be transformed into a random string of characters. This way, sensitive data never leaves the brand, but can still be shared with others for insights.

ID-based solutions certainly seem to be where a sizable proportion of the industry is heading, but, of course, they aren’t the whole picture.



Changes to contextual

As we have seen, in addition to ID solutions and FLoC, over a quarter ([27%](#)) of publishers are considering contextual as an alternative to third-party cookies.

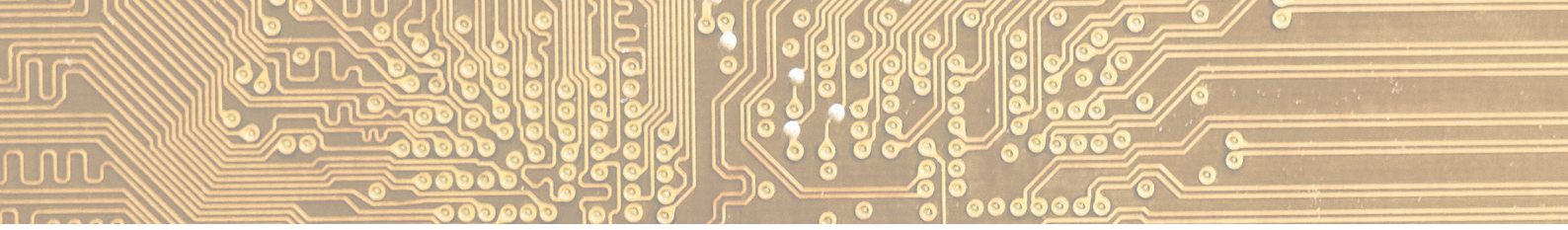
Display ad company, Criteo, for instance, has built its own [contextual advertising product](#) that uses AI to merge content classification with first-party transaction data to better connect consumer purchases with the content they consume.

One area in which contextual finds its strength is video. Online video platform and monetization tool, [Connatix](#), uses natural language processing and computer vision to automatically analyze a publisher's videos. The platform indexes videos and generates contextual metadata, on which buyers can target ads. In an [interview](#) with VideoWeek, David Kashak, Connatix's CEO and Co-founder, said he believes it is not simply the loss of cookies that is driving interest in contextual – it is also performance. *“We’ve been running post-campaign analysis for a lot of companies who have been using contextual targeting, and we’re seeing an uplift in metrics like brand recognition, completion rate, click-through rate and so on.”*

Smart (AdServer) recently acquired fellow French ad tech firm, DynAdmic, which focuses on contextual in video and CTV. Smart believes this will strengthen cookie-free targeting within its own DSP, and has also [partnered with ID5](#) to incorporate Universal ID into their offering.

Meanwhile, media giant, [Verizon Media](#), is also making waves in contextual, building a suite of solutions aimed at supercharging contextual using AI. Part of its ID-free targeted ad solution – Next-Gen Audiences – boasts audiences created from machine learning models built on Verizon's extensive first-party data signals. Enriched by contextual and real-time signals, publishers can use the tool to leverage existing audience data, coupled with predictive audience signals, to improve campaign accuracy and performance.

In summary, publishers are likely to continue to use contextual primarily to enhance behavioral first-party data, especially through the use of AI, rather than as a standalone solution.



Evolving edge computing

Edge computing is definitely an option for those wanting to steer clear of privacy aspersions, although there is little evidence to support any rapid uptake in the publishing industry – significantly, it wasn't included as a contender in the [Teads survey](#). However, with ID solutions yet to be legally tested against legislation such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) – and the increasing deprecation of advertising IDs in GAFA (Google, Apple, Facebook, and Amazon) platforms – edge computing may increase its foothold quicker than we might expect.

Google has [recently hinted](#) that the industry must prepare for an ecosystem where persistent third-party IDs are not acceptable. Google Ad's VP and GM Jerry Dischler, perhaps unsurprisingly, says *“third-party cookies and other proposed identifiers that some in the industry are advocating for, do not meet the rising expectations that consumers have when it comes to privacy. They will not stand up to rapidly evolving regulatory restrictions.”*

As Fosci agrees, *“anything involving exchanges of personal data from one legal entity to another is not compliant or sustainable. In contrast, decentralized solutions that leave personal data on the device whilst building anonymous cohorts are more viable.”*

In conclusion, edge computing may end up becoming the best solution for certain audiences, for example, on Apple devices, but this will take time to materialize.



Next steps for publishers

To prepare for a future without third-party cookies, publishers should take action in the following three areas:

1. Combine data sets as a safety net

From speaking to a cross-section of the publishing industry, it seems the advice remains to continue with a portfolio approach for the time being and focus on combining data sets. As Switzer advises, *“smaller publishers should consider combining data assets and advertising operations with other publishers so that advertisers can buy their audience data at scale. Data is now firmly controlled by the publisher, and giving that control to another party would likely sustain the publisher-unfriendly ecosystem that we have today.”*

If it is normal practice for tech giants (and even marketers are starting to build their own **[‘brand gardens’](#)**), there is nothing to stop publishers creating their own walled gardens. As Fosci suggests, *“publishers should build and enrich their first-party data to drive behavioral and contextual targeting on their site. The next step is to join a publisher walled garden, with companies federating their first-party data so as to create bigger and better audiences that are more attractive to advertisers. Their vision should include building and selling premium audience segments through PMPs and programmatic guarantees without privacy shortcuts.”*

2. Focus on first-party data wherever possible

While combining datasets is a logical next step for publishers, in the medium term it is also worth continuing to build a focus on subscriptions (as per our **[last report](#)**) and other first-party data. As Munchbach concludes, *“Making first-party data a strategic business asset is critically important to mitigate against the loss of third-party cookies”*. Publishers who are unsure how prepared they are for the demise of the cookie can use BlueConic’s aforementioned tool, which provides ‘readiness scores’ based on data confidence, access, and utility – along with detailed steps for how companies can prepare to move away from third-party data.

3. Add a layer of contextual to behavioral

It seems most industry players are largely sticking with what they know – behavioral targeting. However, they're now using first-party data (whether authenticated logins or first-party cookies), enhanced with DMPs and other technologies such as contextual, AI and/or machine learning. It is worth bearing in mind, however, that some audiences could become invisible to these methods, most significantly a proportion using Apple devices. The exact size and nature of these audiences remains to be seen, but they will likely require a different approach to attribution. And, with probabilistic matching not without its challenges, this may be where edge computing flourishes.

Fosci predicts that “contextual targeting will grow, but behavioral targeting will stay, because if it doesn't, the ROAS gap between Facebook/Google and the open web will be too large for anyone to bear. Those who can successfully combine contextual with an ethical, sustainable behavioral strategy will thrive.”

And, as Jules Polonetsky, CEO of the Future of Privacy Forum, sums up, “we're going to see a bifurcated world: hyper-targeted identity-based advertising in places where the channels support it, and then big data-driven advertising – via Google, Apple and the others.”

In a time of huge change, it is worth remembering that brands still need to advertise – and publishers are critical to enabling them to reach their audiences. The future of targeting will be multi-dimensional and savvy publishers need to understand and test out the different approaches now. Only then will they be able to grasp the opportunities available and offer advertisers effective solutions before the end of Google's reprieve.

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 Lexical Llama, Hazel's speciality 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's 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.

