

WITHOUT A TRACE:

*the future of online
targeting beyond
identifiers*



1

FOREWORD

By Carl White, CEO and Co-founder, Nano Interactive

Ask anyone at a dinner party (remember those?) what they think of digital advertising and you are often greeted with an unfavorable response. Dig a bit deeper with people and while they often say they dislike being 'stalked' by advertising, they also understand that a trade-off is made in order for their free - or at least subsidized - content to be produced.

This inherent contradiction and the concurrent need for new ways to adapt to the changes being brought about by the imminent demise of the third-party cookie has created fertile ground for innovation within adtech.

Much of the focus of the digital marketing community in the past 18 months has been on the fine detail. Numerous ways have been developed in which identity proxies can be used to protect the hard-won revenues that have developed for publishers and adtech providers over the past two decades.

Email address-based proxies and first-party data relationships have been a focus of development and discussion within the adtech community. Some clever technologies have been developed to stitch together different identity databases. Doubtless many of these technologies will be successful.

However, in some ways these developments completely fail to see the greater leap that our industry needs to take. Improvements in AI and machine learning, combined with faster processing speeds, are enabling the development of live decision-making techniques and more nuanced content analysis that can facilitate targeting based on the live signals of intent and strong signals of likely mood and sentiment of the user.

Applying these new approaches has been our focus at Nano Interactive for a number of years. We started with the understanding of the live search queries that had delivered users to a particular page at a particular moment. On top of this we have now built exciting next-generation contextual capabilities that understand the underlying meaning and sentiment of a particular page. Combining this multitude of complex live signals without any personal identification of the user has delivered remarkable campaign performance success.

Our goal is to deliver effective digital advertising without the need for any personal identification of users.

2

EXECUTIVE SUMMARY

The online advertising industry is in the middle of the biggest change in its 27-year history. Its underlying approach is moving from one of tracking being the default and privacy being optional, to privacy being the default and tracking optional.

The recent short stay of execution for the 3PC in Google Chrome will give the whole industry more time to find alternative solutions that work best for specific needs. The industry has shown itself to be insufficiently well prepared for the move away from cookie reliance over the last 6 months.

Short delay or not, this change has been building for some time. It came to a head this year because of the 2020 announcement that Google Chrome was implementing an update in order to block third party cookies from its browsers. Suddenly we were faced with the

prospect of cross-site tracking capabilities vanishing from two-thirds of the world's browsers. With Safari and Mozilla having already made the move, this meant only one browser in ten would still accept third-party cookies.

This will affect every aspect of the online advertising ecosystem. Established functionality that will either be lost or compromised includes targeting, retargeting, measurement, frequency capping, attribution, campaign optimization, and dynamic creative optimization. Research by IAB Europe at the end of 2020 found that half of industry professionals felt it was critically important to find a replacement for the third-party cookie. The same research also found that only a quarter (28%) of respondents felt they were either "very" or "quite" prepared for the post-cookie world.

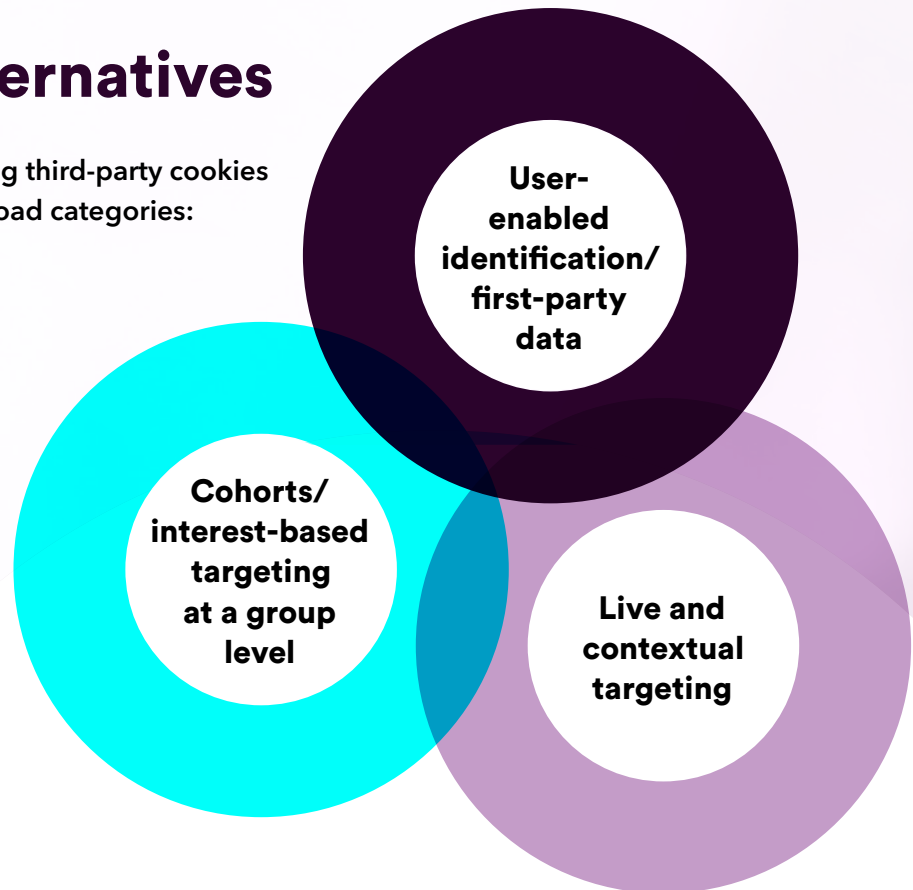


28%

of respondents felt they were either "very" or "quite" prepared for the post-cookie world

The alternatives

Ways of replacing third-party cookies fall into three broad categories:



However, while all of these go part of the way to addressing the problem, the industry consensus is that companies will have to tailor a mixture of all three to meet their individual requirements.

There are more questions going forward. While the use of first-party cookies to improve a user's on-site experience seems likely to continue to be acceptable, the use of anonymized first-party identifiers to replace third-party cookies has already run afoul of privacy campaigners, legislators and Google.

Meanwhile Google is trialing its own replacement, a way of algorithmically building interest-based targeting groups known as FLoC: a Federated Learning of Cohorts. It reports promising results from early simulations, but real-world testing with advertisers only began in Q2 2021.

The continuing trend for greater regulation of online privacy and data security suggests that much of the heavy lifting in ad targeting in the future will be done by new forms of targeting that use no personal identifiers and have a greater reliance on next-generation contextual targeting.

The opportunities

This should not be seen as a backward step. Rather it's an opportunity for the industry to rethink its relationships with consumers, to approach advertising from the perspective of what users need, rather than what advertisers want.

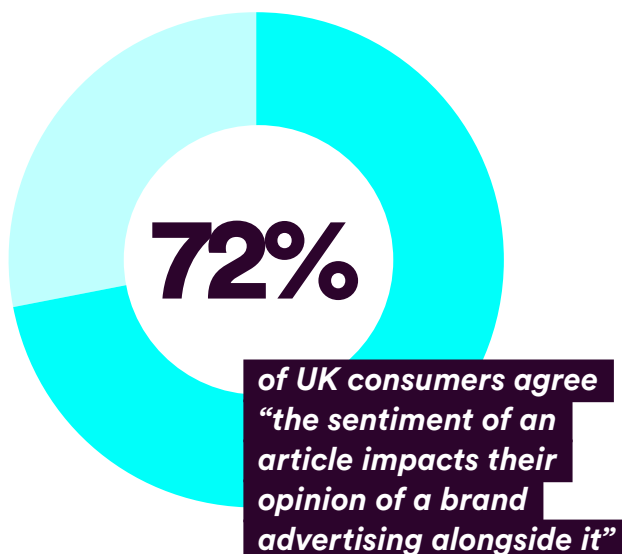
Evidence already suggests people are willing to pay a 'privacy premium' to buy from companies that build greater security and privacy features into their products and services.

Greater nurturing of first-party relationships should allow publisher and advertiser brands to develop a greater understanding of their customers, leading to increased brand affinity, greater earned presence on social media and more collaborative approaches to meeting their needs.

Finally, contextual may be the oldest form of ad targeting, but technology has brought it to the edge of a new era. Analysis of live signals improves the match between user intent and ad placement, therefore leading to performance success. Meanwhile, advances in AI mean that contextual targeting can now understand the underlying meaning and sentiment of the editorial content. Research in 2020 by Integral Ad Science found that nearly three-quarters (72%) of UK consumers agree "the sentiment of an article impacts their opinion of a brand advertising alongside it". In other words, contextual targeting's newfound ability to locate an editorial environment that provides a complementary mood state to an advertising message should further enhance marketing success.

Marshall McLuhan famously stated that "the medium is the message", but next-generation contextual targeting may mean that "the mood of the medium is the message".

All of this means enhanced contextual targeting is likely to be the cornerstone of the privacy-first future.



3

INTRODUCTION

The term one-to-one marketing first came to prominence in 1994, when marketing gurus Don Peppers and Martha Rogers published *The One to One Future*. The development of online marketing so far has been a 27-year pursuit of this ideal.

Now, however, the online marketing industry is approaching perhaps the most important inflection point in its history. The cookie, which coincidentally was also invented in 1994, and which sits behind almost all the targeting technology currently in use, is coming to the end of its time. Or, more precisely, the third-party cookie is. Early next year Google will follow the moves of Apple with Safari and Mozilla with Firefox, and block the use of third-party cookies within Chrome.

According to Statcounter, in March 2021 these three browsers together accounted for 87% of the market worldwide. Chrome alone accounts for 64%, so the impact on all areas of the online marketing ecosystem - publishers, advertisers, agencies and adtech companies - will be hugely significant.



87%

In March 2021 Safari, Firefox and Chrome together accounted for 87% of the market worldwide.



64%

Chrome alone accounts for 64%

Privacy by default

Since the early days of the internet, there has been a tension between consumers' desire for more relevant, targeted advertising, and their suspicion of the technology used to provide it. The balance is now swinging firmly toward suspicion and, ultimately, rejection. As Tina Lakhani, Head of Adtech for IAB UK, puts it: "Tracking used to be the default, and privacy was optional. We're now moving toward a world where privacy is the default and tracking is optional."

A Consumer Reports survey carried out in the US in February 2020 found that two-fifths (40%) of respondents were either "extremely" or "very" concerned about the privacy of the data collected about them by companies, and the same percentage were either "extremely" or "very" concerned about the amount of data collected about them. A further third were moderately concerned about both these issues.

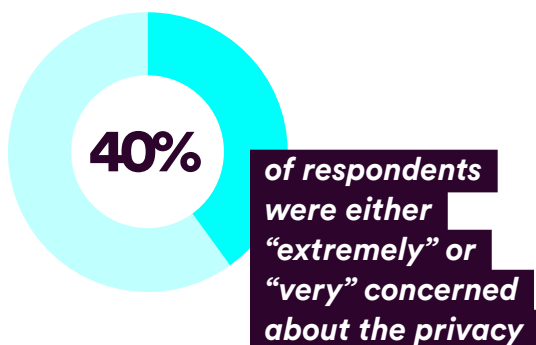
In addition, almost two-thirds (64%) said companies should be prohibited from sharing consumers' personal data with third parties.

However, attitudes to data privacy vary considerably from country to country. In the UK, *Deloitte's 2020 Digital Consumer Trends* survey found that: "UK consumers have

become less concerned about the use of their data: in 2018, 47% of respondents stated they were 'very concerned', this has now halved to 24%." Deloitte attributes this relaxation of attitudes to consumer familiarity with, and acceptance of, the value exchange inherent in online marketing and advertising.

Similarly, the 2020 annual survey by the UK Information Commissioner's Office into the UK population's attitudes to data protection and freedom of information found a decrease of 10 percentage points in the proportion of people with low trust and confidence in companies storing and using their personal information (to 28%) from 2019. But it also found a fall in the proportion with high trust and confidence in the same period, from 32% to 27%.

Before the UK's online advertising industry gets too excited, it's worth noting that any optimism could be based on shaky foundations. The Deloitte researchers suspect most people are unaware of the extent and complexity of data sharing that actually occurs: "The majority of digital users may not be able to comprehend the process via which information such as browsing history, location and device used could be shared instantly with hundreds of third parties."



Legal action

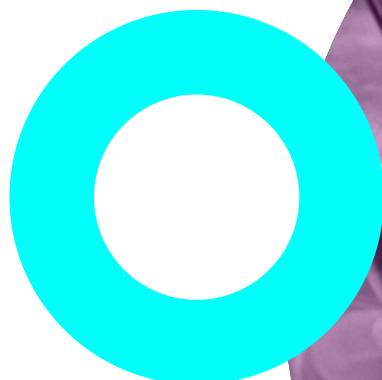
Naturally, public concern is the driving force behind political action. Europe was an early mover in setting up a regulatory framework around individuals' privacy, with the Data Protection Directive in 1995. This was supplemented by the e-Privacy Directive (ePD) in 2002, and superseded by General Data Protection Regulation (GDPR) in 2018.

Since then, similar legislation has come into effect or is being discussed elsewhere.

In January 2020, California's Consumer Privacy Act (CCPA) became law. This operates on an opt-out basis rather than the opt-in of GDPR, but still gives users in the state the right to know what personal information a business collects about them; how it is used and shared; the right to delete personal information collected from them; and the right to opt out of the sale of that information. The CCPA will be supplemented by the California Privacy Rights Act, which is due to come into force at the start of 2023. More than 100 pieces of privacy and data-governance-related legislation have been introduced at state and federal level since the introduction of the CCPA.

Brazil's General Data Protection Law (LGPD) came into effect in September 2020. It is the country's first overarching privacy law, and is based on GDPR. Interestingly, the law defines "personal data" very broadly, to include any information regarding an identified or identifiable person.

Canada's Consumer Privacy Protection Act (CPPA) was introduced in November 2020 and is currently going through the legislative process. The CPPA would update the law around consent to require "that individuals have the plain-language information they need to make meaningful choices about the use of their personal information". Importantly, it also states that de-identified information - personal information with direct identifiers removed - must be protected, and cannot be used without the individual's consent except under certain circumstances.



○ The tech giants respond

Increasing privacy legislation is only half the story. The other half is the way the tech giants, particularly Google, are responding to growing user concern about privacy and data protection.

Google's Privacy Sandbox initiative, announced in January 2020, is intended to "create a thriving web ecosystem that is respectful of users and private by default", according to the company. Google aims to achieve this through a three-pronged approach: replacing the functionality delivered by cross-site tracking, turning down third-party cookies, and mitigating any workarounds to the new functionality.

While browsers are currently in the spotlight, there are also moves in other areas of the adtech ecosystem. In June of 2020, for example, Apple announced that the next version of its mobile operating system, iOS 14, would require app users to actively opt in to be identified to advertisers, replacing the previous default opt-in. iOS 14.5 was launched on April 26 2021 and, according to figures from Flurry, worldwide opt-in rates for cross-app tracking after three weeks were 13%, and only 5% for the US. This clearly shows consumers' lack of enthusiasm for being tracked.

○ Industry concerns

The industry's concern about a replacement for the third-party cookie is partly explained by the number of aspects of online advertising that will be affected by its demise, including: targeting, measurement, frequency capping, attribution, campaign optimization and dynamic creative optimization.

An industry poll by IAB Europe at the end of 2020 showed nearly half the respondents (47%) felt it was "critically important" to find an alternative to the third-party cookie, with just over another quarter (28%) saying it was "quite important".

Strikingly however, the same poll found that only 11% of respondents described themselves as "very prepared" for the post-third-party cookie era, with a further 17% saying they were "quite prepared". This report will look at the online advertising industry's preparations for the disappearance of the third-party cookie. It will examine the solutions being developed to take its place, their advantages and disadvantages. And it will look at the opportunity to step beyond these solutions to create a world where online advertising can be targeted with users at the center and without the need for personal identifiers, cross-site tracking or data sharing.

4

CURRENT SOLUTIONS

“ We’re in a grey area right now as we transition to a world of privacy by default. We don’t know how users will feel when third-party cookies go, and it is up to us as an industry to build and adopt solutions that put consumers and their trust at the heart of everything that we do.

Tina Lakhani, Head of Adtech, IAB UK



Home News Blog Strategy

LATEST ARTICLES

The latest news and trends in business

Ways of replacing third-party cookies fall into three categories:


News Feed
Success Stories
Inspirations
Blog Posts
Our Story

JOIN OUR NEWSLETTER

**Cohorts/
interest-based
targeting at a
group level**


**First-
party data/
user-enabled
identification**

**Contextual
targeting**



First-party cookies are the approach of choice for publishers and brands that have a direct relationship with their readers or customers to the extent that those people will register or sign up for further communications or services, usually with an email address. While this approach explicitly avoids the issue of third-party cookies, there is a problem with scale. Estimates vary, but the proportion of websites with a registered or logged-in audience is generally reckoned to be about 15%, meaning a tiny fraction of the web is available to advertisers based on first-party identification. Even this is misleading, however, since in order to reach that fraction easily, all of them would have to be using the same first-party data solution.

User-enabled identification takes first-party data a stage further. ID technology firms take the personal data supplied at registration, anonymize and encrypt it, and then use it as an identifier for targeting across the existing online advertising ecosystem. The assumption here is that the result of the anonymization process is no longer personally identifiable information, and that therefore rules around PII no longer apply.




This faith may be misplaced. Google announced early in 2021 that it wouldn't build alternate identifiers to track individuals as they browse across the web, and wouldn't use them in its products. The reason given was that: "We don't believe these solutions will meet rising consumer expectations for

privacy, nor will they stand up to rapidly evolving regulatory restrictions.

Certainly, the data privacy laws recently introduced in Brazil and Canada suggest this type of identifier could have a limited future. And it's not just Google the industry needs to worry about when it comes to curtailing cookie workarounds, it seems every Apple IOS update brings forth new challenges for user tracking and IOS15 is no different. A function which allows users to hide their email and IP address could spell disaster for all cookie alternatives which use this as their anchor for identification and to gain consent.

However, this hasn't stopped a multitude of companies from pursuing the Universal ID solution. Numerous players are engaged in a race to find the best alternative, though UID 2.0, the brainchild of The Trade Desk, seems to be the clear front-runner. Already it boasts support from the biggest names in adtech, with Xandr, OpenX, Publicis, Criteo and Nielsen to name but a few pledging support and utilization of UID 2.0.

UID 2.0 is a useful piece of open-source tech and positively highlights the innovative work that can be done when multiple players from all sides of the table come together. However, impressive as it is, it doesn't address the real issue of whether consumers will be happy with an identifier that potentially gathers and merges data from multiple sources, and is anchored by their (very identifiable) email address; anonymized data handling or not.




“ *Universal ID solutions replace cookies, which are more anonymous than an email, by asking consumers to share an email address. The likelihood that someone’s more likely to want to use a personal email address to identify themselves versus a cookie is questionable, so it doesn’t really solve the problem of privacy.*

Matt Morgan, Managing Partner, Head of Product, Dentsu

In addition, privacy advocates are questioning whether the terms under which companies currently collect first-party logins legally permit the data to be used to create alternative identifiers. In this view, the fact that a user has consented to having their data used for marketing purposes does not extend to it being used for cross-site targeting.

“ *What’s going to change for us in re-targeting is that, rather than marketing technology owning the relationship with our anonymous users, we want to take ownership of that relationship. We’re thinking about how we can provide those users with a value exchange that they understand, and that they’re happy to provide their data for alongside their consent. So we’ll say, if you identify yourself, we’ll provide you with something really personal, really valuable, and we’ll market to you with that type of content through various channels, such as email.*

George Montagu, Data Governance Manager, FT.com



Contextual targeting is the oldest form of media targeting. It was the basis of most targeting of traditional media advertising, and in essence is no more complicated than placing a car ad on the motoring page of a newspaper.

The approach retains considerable power with consumers, a fact that has been somewhat lost in the scramble for personalization in recent years. According to The Power of Context report from Integral Ad Science, published in October 2020, almost three-quarters (72%) of UK consumers feel it's important that ads are relevant to the content of the page on which they appear. Nearly as many (70%) say their perception of an ad is impacted by the surrounding content, and two-thirds (65%) have a more favorable opinion of brands in contextually relevant ads.

Modern contextual targeting adds to this by using artificial intelligence to understand the content of a page at a deeper level, beyond simple categories and keywords. This includes understanding the sentiment of the content, from positive to negative.

This has several major implications. Firstly, the IAS research also found almost three-quarters (72%) of respondents agree that "the sentiment of an article impacts their opinion of a brand advertising alongside it".

Simply making sure your ads appear next to positive content should improve consumers' perception of your brand.

Secondly, it improves targeting. For example, a mobile phone manufacturer could target content expressing negative sentiments about rival products.

Finally, it opens up more inventory. For example, if clients only want to be next to positive content they might exclude Covid news. But because there is so much Covid coverage out there, taking it all out of consideration would reduce the scale available to a campaign, and take the brand away from topics which are relevant to people right now. Sentiment targeting means a brand could only exclude negative stories about the pandemic, but still appear next to positive coverage, such as the success of vaccines. In other words, sentiment targeting ensures advertisers know content is not just brand-safe but brand-suitable too.


The drawback of modern contextual targeting is that the metrics available tend to be brand- rather than performance-focused, compared to those available with third-party cookies. Because the approach involves no individual identifiers, it also means that cross-site retargeting is no longer possible, as users of Safari and Firefox should already have noticed.

No silver bullet

This all adds up to the fact that there is no single, simple replacement for third-party cookie-based ad targeting. Companies will have to use combinations of all these approaches, based on their relationship with their customers (and prospective customers). Publishers, and brands that already sell direct, should be improving and explaining the value exchange on offer, encouraging customers to sign up for their

communications and services, and building up their first-party data sets.

Brands that sell through middlemen should be looking to establish direct-to-customer channels, such as subscription services or their own e-commerce offerings. They should also be assessing which parts of their current advertising rely on third-party cookies, and thinking about alternatives.



“ We’re not necessarily trying to replicate retargeting, but that could end up being one of the things we do. There’s no way to know at this stage. We’re trying to understand if there is something that could work from a business perspective, while making sure our users are taken into consideration. We don’t want to find a solution that, even if it’s GDPR compliant, our users aren’t happy with.”

Giulia Rozza, Marketing and Technology Manager,
B2C Marketing, FT.com

5

THE OPPORTUNITY TO GO FURTHER

While companies across the online advertising ecosystem prepare for the post-cookie world, it's important to remember that this is only a means to an end. People are concerned about the way their data is collected, stored and used to track their online behavior. Removing the third-party cookie is simply the way legislators and big tech companies have chosen to address these concerns. But if this doesn't work

- if people continue to feel they're being tracked, whatever the technology used - these gatekeepers have made it clear they will continue to act. And consumers themselves will increasingly opt out of all communication from brands via the 'nuclear option' of installing ad blockers. Data from Statista shows 27% of US internet users now have ad blockers installed, up from 21.5% in 2016.



27%

*of US internet users
now have ad
blockers installed*

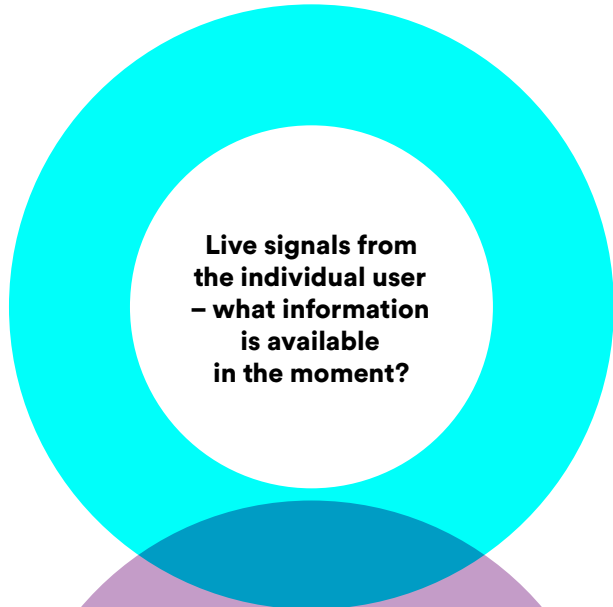
A world without identifiers

Interviewed on MadisonAlley.tv in April 2021, AppNexus Co-founder and former CEO Brian O’Kelley was asked about identity after the demise of the third-party cookie. His response: “Given regulatory frameworks and tech... do we really want to fight this fight, or should we go think about how to make advertising effective without personal identification?”

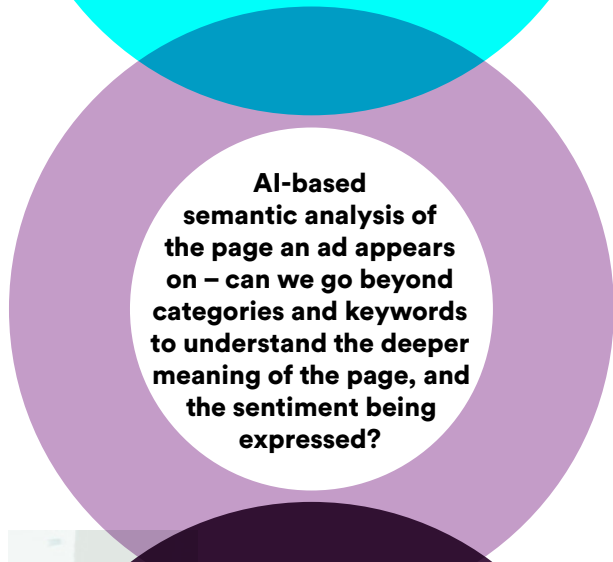
There are two key questions about online advertising without identifiers. Is it possible? And what would the impact be?

This is an area that Nano Interactive has been investigating for two years. The company believes building on contextual technology can make identifier-free targeted online advertising a reality.


There are three elements to its approach:



Live signals from the individual user – what information is available in the moment?



AI-based semantic analysis of the page an ad appears on – can we go beyond categories and keywords to understand the deeper meaning of the page, and the sentiment being expressed?



Zero-tracking measurement – creative performance/ probabilistic measurement/ page-level measurement





Live signals: The most important of these is the search term that brought the user to a particular page and where they came from. Importantly, this includes whether the user came via Google. Nano is the only platform able to use searches performed in Google to target users outside of the search giant's closed ecosystem.

This is supplemented by elements taken from the programmatic bid request, and other non-identifying information including date, time, location and type of device used.

Semantic analysis: AI enables contextual targeting to go beyond simple category- or keyword-matching. Entity salience analysis recognizes the 'things' mentioned in a piece of text (entities) and ranks them according to how significant they would be for a human reader (their salience).

It also allows the sentiment of the text to be assessed on a scale from totally positive to totally negative.

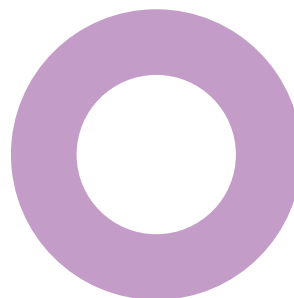
This ensures brand safety, and means targeting can be much more nuanced than previously. For example, it allows targeting by negative sentiment. The UK government recently used this approach to target ads for its Covid vaccination program to people reading articles that were skeptical about vaccines.

Measurement: There are two options for measurement without tracking of individuals, depending on the advertiser. The first is placing a macro into the ad itself, which measures how that particular creative has performed: where it appeared, how long it was viewable for, did something happen as a result of the ad being seen.

The second is through a probabilistic performance graph, based on machine learning. It is possible to know which ads are appearing where, so machine learning is able to make assumptions about whether an action taken at a particular place and time is the result of someone seeing an ad.

Another result of not tracking users is a change in the metrics available. These are more brand-oriented, including viewability and brand impression time. If the advertiser allows the placement of a macro, dwell time can also be measured (the amount of time spent on the advertiser's site as a result of a click-through from an ad).

Changes in the way measurement is performed will place a greater emphasis on an advertiser being willing and able to share information in order to optimize campaign performance.



6

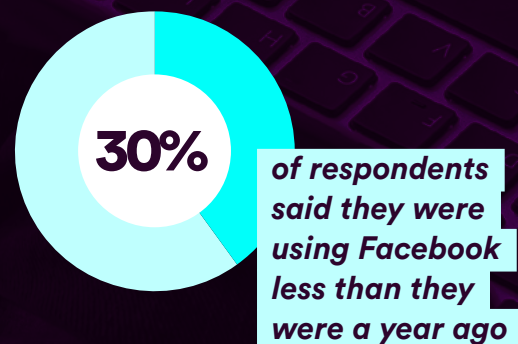
THE IMPACT OF IDENTIFIER-FREE TARGETING

This modern approach to contextual targeting, employed programmatically, offers advertisers a way to achieve the scale once offered by third-party cookies. A user who isn't cookied, or identified through some other means, is invisible to advertisers. In a world without individual identifiers, contextual targeting will be the only proven way of making all these invisible users visible across the open web. Since this is where they spend the majority of their time (more than 56%, according to IAB Europe), it's clearly vital for advertisers to be able to deliver targeted ads on open web properties. It should also increase the amount of inventory publishers can sell.

There is also evidence that consumers are more curious and more attentive when browsing the open web, compared to when they're within the walled gardens of Google and Facebook. An Open X/Harris Poll survey, *The Open Web Vs The Walled Gardens*, published in 2020, found that the majority of people using the open web (58%) were "curious and in a mood to learn more", compared to 39% on YouTube, 32% on Amazon, 24% on Facebook and 22% on Instagram. In addition, when looking for a

business, or for products to buy, two-fifths (80%) of respondents turn to the open web first.

The research also found that the open web audience, which it concludes are in the perfect state of mind to receive an ad, is likely to grow in size. Almost a third (30%) of respondents said they were using Facebook less than they were a year ago, compared to 8% who said they were using the open web less. On top of that, respondents were four times more likely to say they'd use the open web more in the next 12 months than use it less. In contrast, more people said they expected to use Facebook and Instagram less in the next 12 months than expected to use it more.



More is less


There is also evidence that more data for targeting isn't leading to better results for marketers. Writing for Forbes last year, campaign auditing expert Dr Augustine Fou noted that studies showed: "Having hundreds of additional data points to use for targeting ads did not yield a measurable increase in business outcomes. Combined with supply chain costs, data quality issues, ad fraud, and viewability issues, dollars spent in programmatic adtech channels often yield negative ROI."

In other words, by removing data collection and its associated costs from the equation, identifier-free targeting should deliver similar scale to the cookie-based approach, in advertiser-friendly environments, for a reduced investment while not alienating customers.

The benefits of being privacy-first
Beyond the direct impacts of identifier-free targeting, there are broader benefits for both publishers and advertisers in being seen to be taking customers' data privacy and security concerns seriously.

Firstly, as the Consumer Reports Privacy Front & Center research from 2020 found, US customers are willing to pay more for better privacy features across both hardware and software products. The report concludes: "Health, technology and security companies that prioritize consumer privacy and data security should see significant upside."

Secondly, greater nurturing of first-party relationships should pay off in a number of ways for both publishers and advertisers. It should allow brands to develop a greater understanding of their customers, leading to increased brand affinity, greater earned presence on social media and more collaborative approaches to meeting their needs. In 2019, for example, Coca-Cola North America launched the Coca-Cola Insiders' Club, which, for a \$10 a month subscription, sent club members samples of three new drinks a month. The initial 1,000 memberships sold out in three hours.

 *An ideal solution would be for brands to understand that data can be used for enjoyment rather than just exploitation. Spotify's campaigns and its approach to curating playlists, for example, they're personal and they're beneficial to the user. That's where things get interesting in any category, because if you can come up with a solution that benefits both parties, and there's a mutual agreement on it, then you can do things for the greater good.*

Pollyanna Ward, Head of Paid Social, Social Chain, Wickes

7

CONCLUSION

In truth, the fight to preserve tracking-based online advertising has already been lost. The industry has failed both to explain the value it delivers to consumers in return for their data, and to be transparent about how that data is collected, stored and used.

In addition, it has ignored the words of G.M. O'Connell, Founder of the world's first interactive marketing agency, who back in the late 1990s said: "You can't annoy people into liking you." Instead, the industry largely chose to respond to consumers' lack of interest in its intrusive, annoying, irrelevant ads by making them bigger, more intrusive and more annoying, and only a little more relevant.

That era of internet history is now coming to an end. Legislators and some of the world's most powerful tech companies have listened to people's concerns and done something about them. From 2022, many of the targeting tricks up the industry's sleeve will no longer work. For many more, it's only a matter of time.

As Brian O'Kelley says, the industry has a choice. It can carry on fighting a rearguard action against the changes now happening. Or it can think about making advertising effective without personal identification, because that's what its customers want, and its clients need.



8

THANKS

The Drum would like to thank the following people for their help in compiling this white paper. They were not asked to endorse Nano Interactive's products, nor should the appearance of their comments in this report be construed as them doing so.

- **Tina Lakhani**
Head of Adtech, IAB UK
- **El Kanagavel**
Managing Director of Performance Technology, Dentsu
- **Matt Morgan**
Managing Partner, Head of Product, Dentsu
- **George Montagu**
Data Governance Manager, FT.com
- **Giulia Rozza**
Marketing and Technology Manager, B2C Marketing, FT.com
- **Pollyanna Ward**
Head of Paid Social, Social Chain, Wickes