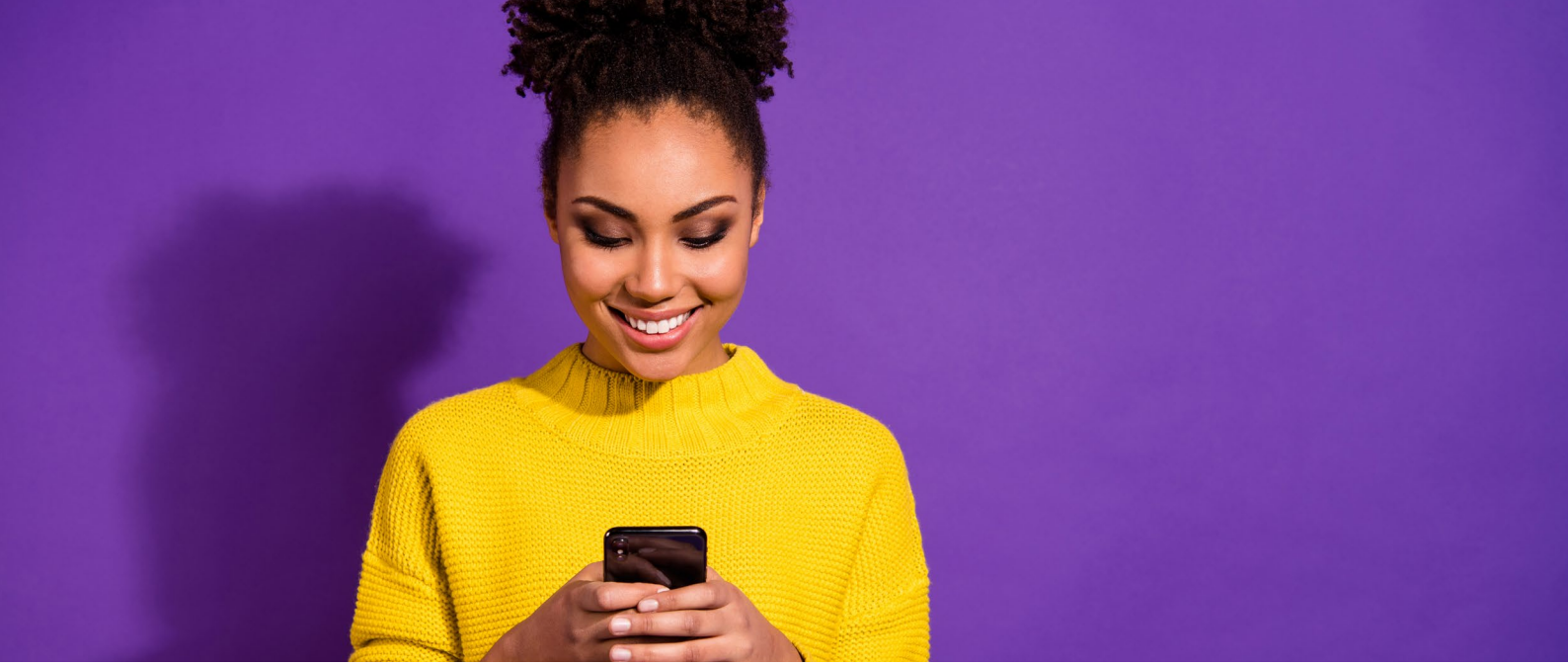
SMARTFRAME

The Rise of Contextual Targeting in a Cookieless World



Contents

Browsing the digital version of this guide?
Simply click on the section you would like to visit.

1.

Executive summary

Third-party cookies are soon to be a thing of the past, and behavioral-based targeting will become less straightforward as a result of this. This in turn underlines the need to explore new ways of delivering advertising to the right audiences in a regulatory-compliant manner.

Third-party-cookie advertising underpins many ad models, so workable solutions are timely and potentially set for widespread adoption. But the need to respect online users' privacy and adhere to the necessary regulations, while ensuring that advertisers gain real benefits from such models, is far from straightforward. Sub-optimal solutions may, at best, be a waste of advertisers' time and money. But, at worst, they can impact the way a brand is perceived, and have serious financial consequences as a result.

Contextual targeting, which works by assessing an online environment in which an ad can be displayed to determine which specific ad is served, is now attracting increasing attention as third-party cookies are phased out. While the concept of contextual targeting is not new, the need to move away from behavioral targeting should ensure that we see plenty of innovation in this space over the coming years. And with the contextual market projected to be worth $376bn by 2027,[1] the incentives are certainly in place.

This paper begins by examining what's led up to this point, before looking at the ways in which today's contextual targeting systems work. It explores how images play a part in contextual targeting, as well as the role and limitations of AI-based technologies when dealing with images, and where this ought to be balanced with human intervention.

It then takes a closer look at the ways in which relevant parties – from publishers and advertisers to online users – stand to be affected by contextual targeting, and how alternative systems may themselves develop in the future. Finally, it examines the growing role of attention as a key performance metric, and the way in which the market is expected to develop over the next few years as contextual targeting gains prominence.

2.

What's changing – and why

Understanding why focus has shifted away from behavioral targeting and towards contextual targeting over the past few years requires us to look at the role of cookies – specifically, third-party cookies.

Third-party cookies, also known as tracking cookies, are pieces of code that are generated as a user navigates between different online environments. By remembering where and when a user has been online, this information can be used to target them based on their behavior, and retarget them with advertising related to a previously visited website.

In practice, for behavioral targeting, this helps to build a profile of the user based on their habits so that messages can be better targeted to their interests. For retargeting, meanwhile, looking at a pair of shoes online on one occasion, for example, may lead to an ad for that store or brand – or even those specfic shoes – being served at a different day and time, on a completely different website.

For the advertiser, these approaches have obvious appeal. It targets based on user interest and intent, and reminds users of something they may potentially be interested in when their focus is elsewhere. If you already know that a user has expressed an interest of some sort in a product or brand, it follows that they would respond better to advertising than someone who has never expressed any interest or behavioral intent at all.

The downside to this is that it leads to incongruous online environments in which the content of a webpage may bear no relation to the advertising being served alongside. Not only does this stand to affect the user experience of that website (and, potentially, the image of the brand), but it also serves as an uncomfortable reminder that a user's online activity has been monitored by an unknown third party.

Over the last few years, collecting the data associated with these cookies has been complicated by the introduction of various regulations regarding the ways in which information that may be used to personally identify individuals can be collected and

processed. To some, this appears as a response to well-publicized scandals involving data collection and privacy, most notably the Cambridge Analytica affair that came to light between 2015 and 2018. The reality, however, is that discussions around the suitability of existing directives and regulations to ever-changing online spaces were being had long before these scandals had been uncovered.

For example, the Data Protection Directive (Directive 95/46/EC), enacted in 1995, detailed the ways in which personal data should be processed and transferred within the EU. As a directive rather than a set of regulations, it allowed individual countries to set their own laws based on these guidelines, which led to complications around data collection and transfer between different territories. It wasn't until 2012 that the European Commission started to discuss the idea of unifying all of these different rules under a new set of regulations named GDPR, but the intervening years saw the introduction of various other directives related to privacy and data processing. These include the ePrivacy Directive (ePD) in 2002, which was followed up by an amendment in 2009 and subsequently referred to as the 'EU cookie law', as well as the Privacy and Electronic Communications (EC Directive) Regulations in 2003 (PERC), which was most recently amended in 2019.

GDPR, along with a new UK-specific Data Protection Act, came into force in 2018. Two years later, as the UK began the process of leaving the EU, elements of the two were combined to create UK GDPR. Today, UK GDPR and the Data Protection Act 2018 continue to be in effect alongside PERC.

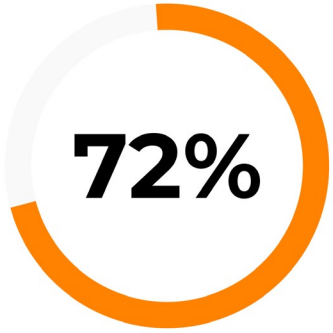
Has GDPR been effective?

In the four years since GDPR came into force, a number of companies have fallen foul of its regulations and have been hit with significant fines. In 2021, Amazon was fined €746 million for unspecified alleged breaches of GDPR.[3] Later that year, the Irish Data Protection Commission imposed a €225m penalty on WhatsApp for allegedly failing to explain its legal basis for certain data processing,[4] while Google LLC and Google Ireland were fined a total of €150m for making it difficult for users of google.fr and YouTube to refuse cookies.[5] This was two years after Google had been fined €50 million for the wording within a privacy notice made available to its users, together with the way in which the company requested their consent for personalized advertising and other types of data processing.[6] Other companies that have had to pay eight-figure fines as a result of GDPR violations include British Airways, H&M, and Marriott.[7] While some of these fines may appear to be excessive, the fact that UK GDPR allows fines of up to £17.5 million – or 4% of the company's global turnover, if this is greater – means that it's the biggest companies that end up facing the harshest penalties.

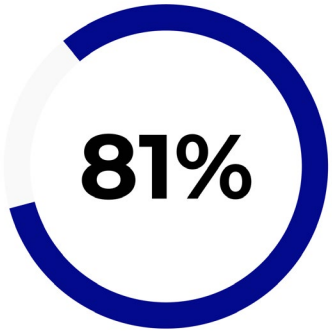
EU GDPR and UK GDPR place limits on the extent to which data can be collected and require users to be notified of the data that is being processed when they visit a website. As these regulations came into force, website operators had to make sure that, among other things, non-essential cookies were not enabled by default, while companies behind popular web browsers drew attention to existing means by which tracking cookies could be removed, eventually introducing cookie-blocking features that would later be enabled on their browsers by default.

These changes, and the publicity around them, have made online users more aware of the collection of their personal information and the steps that they could take to protect it. Privacy-focused browsers have now become the norm, while VPNs are widely used around the world. Search engines that promise not to track user activity have also risen in prominence.

The consequence of this is that, as there is less data available on which to base targeting decisions, behavioral-based targeting models have ceased to be as effective as they once were. As a result, the advertising industry has been forced to consider alternative ways in which they can reach relevant audiences while respecting their privacy and complying with relevant regulations. Alongside this, changes in the habits and expectations of online users, together with the growing use of mobile devices for online browsing, have also caused them to carefully consider the advertising solutions that are fit for the future.



Percentage of people who feel that almost all of what they do online is being tracked by advertisers, technology firms or other companies [2]



Percentage of people who say that the potential risks they face because of data collection outweighs the benefits [8]

Similar regulations around the world

EU GDPR and UK GDPR only concern the EU and UK respectively, but similar regulations regarding the protection of personal data have been introduced in many other countries. These include South Korea's Personal Information Protection Act, the California Consumer Privacy Act of 2018 (CCPA) in the US, the Lei Geral de Proteção de Dados (LGPD) in Brazil, and Thailand's Personal Data Protection Act BE 2562 (2019) (PDPA).

1995
Data Protection Directive adopted

2002
ePrivacy Directive (ePD) comes into effect

2003
The Privacy and Electronic Communications Regulations (EC directive) 2003 comes into force

2009
ePD is amended

2012
EC announces plans to unify data protection laws across the European Union via new regulations called GDPR

2016
GDPR is adopted

2017
Apple introduces Intelligent Tracking Prevention (ITP) for its Safari browser

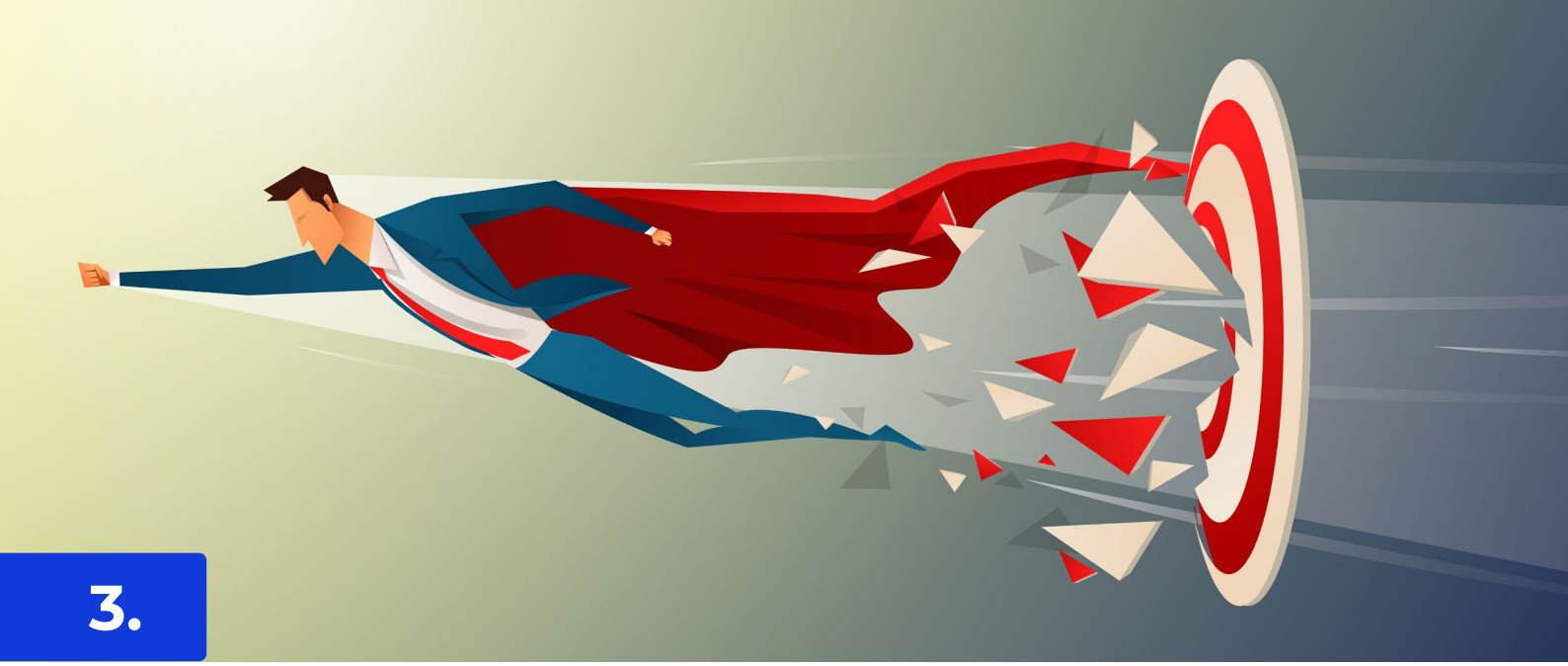
2018
GDPR becomes law | UK announces Data Protection Act (UK GDPR) | California Consumer Protection Act (CCPA) is passed by the state legislature | Mozilla releases Enhanced Tracking Protection for its Firefox browser

2019
Mozilla announces that Firefox will block tracking cookies by default

2020
CCPA comes into effect | Apple updates its ITP feature to block all third-party cookies by default | Google announces plans to scrap third-party tracking cookies in Chrome | UK GDPR comes into effect

2021
Google announces that it's to start testing a new interest-based tracking system called Federated Learning of Cohorts (FLoC)

2022
Google scraps FLoC and proposes a new system called Topics



3.

The rise of contextual targeting

Contextual targeting may be receiving increasing attention today, but it's something that has been with us long before the internet.

Holiday packages being advertised in the travel section of a newspaper, for example, is a straightforward example of contextual targeting. Online, however, the principle makes use of many additional data points and AI tools for a considerably more sophisticated solution.

Percentage of UK consumers who say that ads are more likely to be remembered if they appear next to content that is relevant [12]

How is contextual targeting different from behavioral targeting?

The most obvious difference between contextual targeting and behavioral targeting is that contextual targeting serves advertising that is relevant to the environment in which it's viewed, whereas behavioral targeting serves advertising based on a user's previous online activity.

This difference is important for three key reasons. First, it's reasonable to assume that a user browsing a particular website may be more receptive to advertising related to its content. Those same adverts for holiday package deals, for example, would be a natural fit on a tourism website or a travel blog. And consumers themselves appear to prefer this; a survey conducted by the Interactive Advertising Bureau (IAB) showed that 81% of UK consumers prefer online ads to match the content they are viewing.[9] From an advertiser's perspective, this increases the chance of it resonating with that particular audience, and with it, higher click-through rates and a better ROI.

The second reason is related to all of this. Contextual targeting serves ads that are relevant to the there and then. In contrast, behavioral targeting's approach of using information from previously browsed websites can be both a strength and a weakness.

Its strength lies in the fact that it may remind a user of something no longer at the forefront of their mind, which may well facilitate a conversion at a time when it otherwise wouldn't happen.

But its weakness is the risk of serving ads that are no longer relevant to the user. Would a user have any interest in seeing package holiday deals once they had returned from holiday? It's unlikely – but the behavioral targeting system wouldn't necessarily appreciate this.

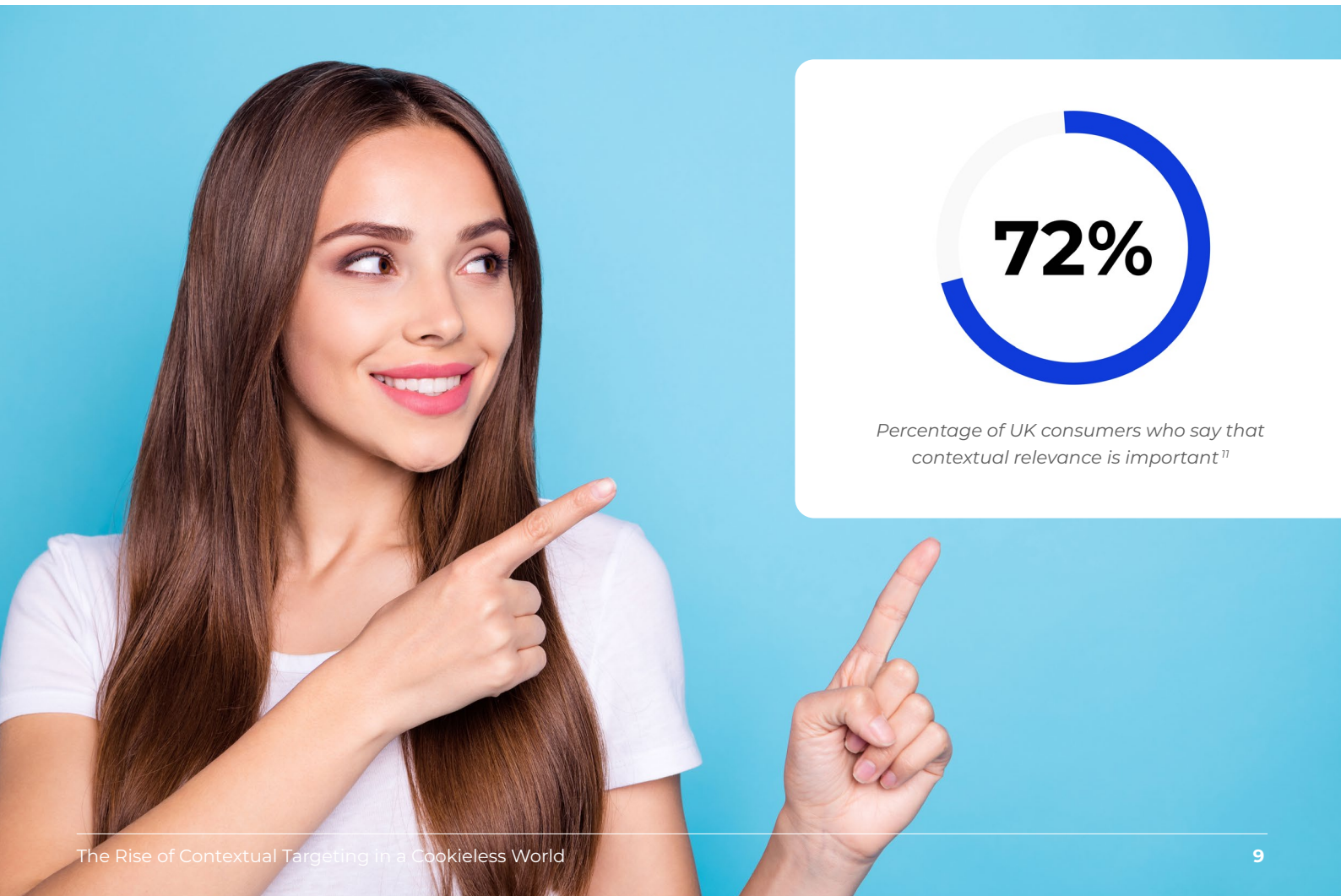
Third, by placing contextually relevant advertising alongside this kind of content, the user stands to have a more positive experience with that brand. The same survey showed that 65% of UK consumers have a more favorable opinion of brands that serve contextually relevant ads.[10]

Going further

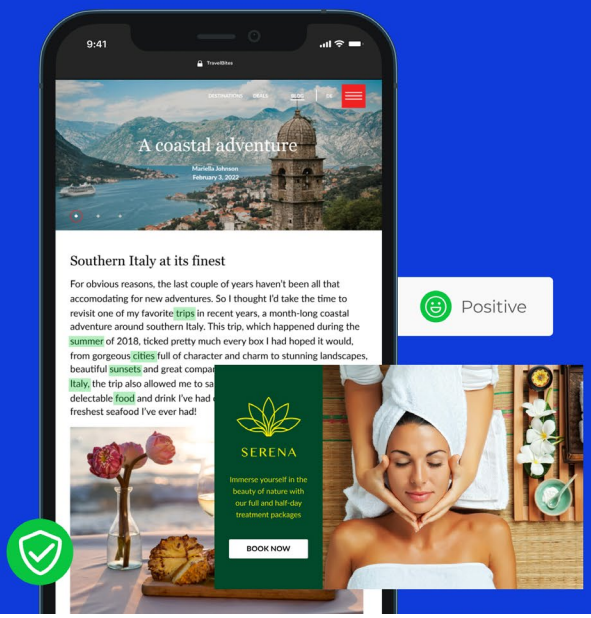
Today's contextual targeting solutions are particularly comprehensive. While keywords and topics are still central to today's contextual targeting solutions, modern systems allow for a considerably more nuanced reading of the webpage, and for ads to be better tailored to a specific audience.

For example, rather than just taking contextual signals from keywords, topics, and URLs, semantic and natural language processing allows for contextually relevant phrases, sentiment, and tone of voice to be detected – and all of this can shape the type of advertising that would be most appropriate to serve.

The ability to spot problematic content and sensitive subjects, and to match this with prohibited topics, can also help with brand safety. Together with language, geolocation, and other factors, these all come together to deliver a highly informed targeting solution, all while respecting user privacy.



Percentage of UK consumers who say that contextual relevance is important[11]



Subject recognition can be used to determine subjects and other elements within the image, and this provides additional contextual signals to keywords, topics, sentiment, and so on.

How do images play a part?

Images can make up a considerable proportion of a page's content, and today's contextual targeting solutions can take advantage of this.

First, subject recognition can be used to determine subjects and other elements within the image, and this provides additional contextual signals to those described above. These signals can be used to determine the kind of advertising that's served alongside the images, which makes these ads contextually relevant to their environment.

Second, by using the image as a frame for the advertisements, these stand to be more prominently displayed than conventional display ads, such as banner ads that may lie above, below, or to the side of content. The issue of banner blindness is well understood.

Given that such images are part of a page's content, rather than conventional advertising that's served *in addition* to this content, any advertising displayed here gives the impression that it naturally belongs to the content the user is interested in.

Does everyone benefit?

As we have seen, online audiences benefit from both the relevance that contextual advertising can bring them and more congruous online environments. But how do advertisers benefit?

From the advertiser's perspective, rather than just serve as a regulation-compliant alternative to behavioral targeting, contextual targeting allows audiences to be served ads when and where they are likely to be receptive to them.

When combined with the principle of in-image advertising, not only does the advertiser gain a broader range of contextual targeting signals for more relevant ad delivery, but also the potential of better ad visibility than usual thanks to in-image ad placement.

It's not just advertisers, however, that need to consider how best to take advantage of contextual targeting as third-party cookies are phased out. Publishers also need to discover new ways of monetizing their products, particularly those that lack some kind of subscription service to their online properties.

Increasing the relevance of advertising encourages audiences to develop trust with their brand. Combining this with innovative ways of displaying images – such as image streaming – also allows for the introduction of additional engagement-boosting features, which help to increase dwell times and brand loyalty. Publishers that do this while collecting better-quality first-party data stand to benefit even further.

Contextual advertising in images does introduce additional issues, however, and these need to be addressed if brands are to rely on this system. These are discussed in the next section.

4.

Not all in-image ad tech vendors are created equal

Images are deemed to be an important part of contextual targeting, not only as a source of data to help determine ad selection, but also to provide a frame for high viewability. In the absence of third-party cookies to facilitate tracking specific users, the ability to decipher the content of an image, find the relevant ad, and serve it in a highly visible location – and all within split seconds – has clear appeal for advertisers.

But in order to ensure brand safety, ad relevance, the avoidance of legal issues, and other key factors that make any such solution viable, ad tech companies need to consider several important factors.

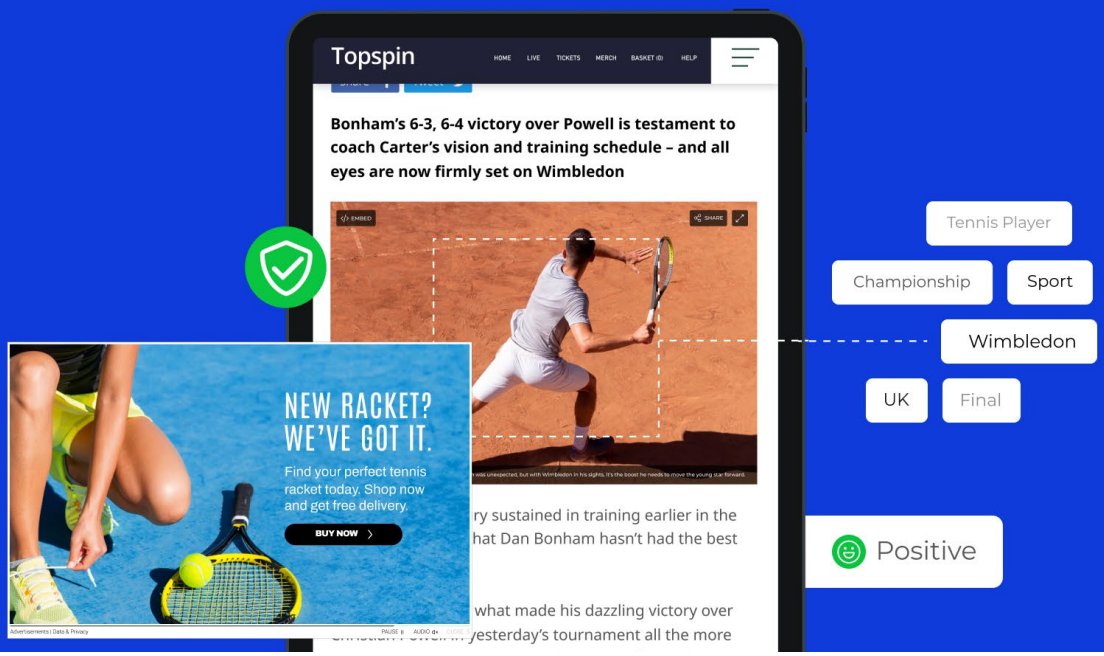
Competence of existing AI solutions

There's no doubt that today's AI-based tools that use subject recognition to determine what's in an image are sophisticated. But where might such systems fall short?

One area is the accuracy of subject detection. Incorrect subject detection may weaken the relevance of the ad deemed to be suitable, or may lead to something inappropriate being shown, which may call the reputation of the brand into question. While this may be less of a concern with professionally captured images, where clarity, focus, exposure, and other factors will be carefully considered by a skilled photographer, the overwhelming majority of images online are not captured with this level of care, which results in a less-than-perfect starting point for accurate subject recognition.

Brands have an interest in keeping their brand safe and away from undesirable content, whether this is something inside an image or the environment in which an advertisement is displayed. The blocking of sensitive and potentially problematic categories can help to some degree, but wherever an element of guesswork is involved, the risk of a bad match – and with it, compromised brand safety – remains.

SmartFrame's approach to this is to rely on as much verifiable information as possible and to limit the extent to which AI is allowed to make key decisions, particularly those that could harm a brand's reputation or a user's safety. In the context of images, SmartFrame's solution makes extensive use of image metadata that has been determined by the owner of an image or the library that owns its rights. By doing so,



SmartFrame can be sure of what the image contains, and this helps to ensure that ads matched to it are appropriate.

There's a further good reason for basing decisions on metadata rather than AI-powered subject recognition. Forming a deeper understanding of what's going on in the image can be used to hone the advertising that's served alongside it.

For example, let's suppose we're dealing with an image taken at a sporting event, such as a soccer game. A solution based entirely on subject recognition may be able to determine that the image shows a number of people, a soccer ball, grass, sports clothing, and so on. It may be able to extract text from the image (such as the team's sponsor) and may be able to determine expressions and the overall sentiment from the players' faces.

What it may not do, however, is tell us which specific players are involved, where the game is being played, which teams are involved, and so on, details that may all be known by the photographer or image rights owner.

These kinds of details are typically included within image metadata. Having access to this allows SmartFrame to provide greater context for the image, which better informs its suitability to be associated with specific advertisements.

Association

Even if a subject is correctly identified by subject recognition, the process of serving advertising within it can create complications.

Most in-image advertising takes the form of a small banner, which is typically placed alongside the bottom of the image. Viewed individually, an image and the ad served within it may appear to be harmless. But when displayed together, this may not necessarily be the case.

Why is this? Let's consider an image that shows a celebrity or another public figure. It may be the case that the celebrity has been paid to endorse a particular brand of clothing, jewelry, or perfume, but the ad that ends up being served within it is from a rival brand. As neither the subject nor the brand may be deemed problematic on their own, and given that the possible combinations of subject and advertisement are essentially endless, there is no practical way of avoiding this from happening. But this association could easily be construed as a promotion of the brand by the public figure, which could potentially lead to legal action from a brand with which the subject has some kind of agreement.

Even if such a system was in place, the fact that public perception of brands, individuals, and products are not fixed but subject to constant change would make it completely impractical to keep it up to date.

SmartFrame's solution to this is to momentarily display the ad over the entire image, rather than to display a small banner for a period of time alongside it. This solves the association issue

described above, but it also delivers additional benefits to advertisers. The most obvious of these is the fact that the advertisement is displayed considerably larger than usual. Not only does this help it to be more visible, but it also allows for greater flexibility with respect to copy, graphics, images, and CTAs, increasing its potential impact.

As SmartFrame images are streamed, they can also be delivered at a much higher resolution than would otherwise be the case. Features such as Hyper Zoom, meanwhile, encourage interaction and increase overall engagement of the advertisements laid over them.

Furthermore, as the SmartFrame image and advertisement are served in one cohesive unit, it's easy to program the latter in such a way that it only fires when it's in full view, where it is far more likely to attract the viewer's attention. Where there are multiple SmartFrame images on one page, the most prominent image can also be chosen to serve such an advertisement, further increasing its visibility.

How does in-image contextual targeting benefit everyone involved?

Online users:

- enjoy more cohesive online environments
- have their privacy respected
- see relevant ads when they expect to see them

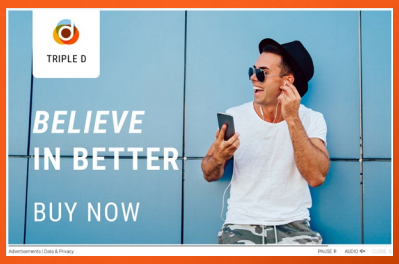
Publishers:

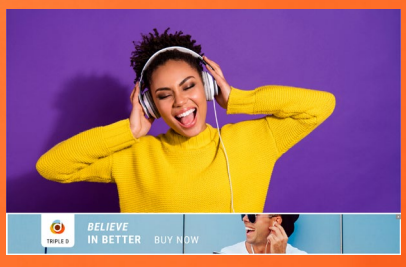
- improve the user experience for their audience
- monetize site traffic
- gain new revenues from the display of in-image ads

Advertisers:

- serve relevant ads
- enjoy prominent placement and large ad displays
- more easily comply with necessary regulations

SmartFrame's in-image advertising solution displays the ad over the entire image for a set period of time, rather than as a small banner within it, which helps to maximize its impact.





5.

What are the alternatives?

Contextual targeting may be growing in prominence, but other options either exist or are currently being proposed. So what are the main alternatives we should be focusing on?

Google's Privacy Sandbox

Google knows better than anyone else about the need to replace third-party cookies with futureproof, privacy-focused alternatives. But it has made it clear that such alternatives need to be in place before third-party cookies can be retired. This explains why it has not yet followed other browser providers such as Apple and Mozilla in removing third-party-cookie support from Chrome, which today accounts for around two-thirds of all web traffic.[13]

Its answer to this is the Privacy Sandbox initiative. Announced in 2019, Google states that the aim of the Privacy Sandbox is to develop new technologies that allow for greater privacy for individuals, introducing tools that will make third-party cookies obsolete, while allowing publishers and developers to keep their sites free by continuing to serve cookie-free adverts.

Additionally, the initiative aims to block or limit covert tracking methods, such as fingerprinting (discussed below), and to collaborate with others to develop industry-standard tools.[14]

One of the tools that came as a result of this initiative was called Federated Learning of Cohorts (FLoC), which was based on the principle of grouping people into cohorts for the purpose of ad targeting. The response to this was negative from many other browser providers, privacy groups, and others, some of whom questioned its compliance with regulations such as GDPR among other things.[15] Ostensibly as a result of this reaction, Google ceased the development of FLoC in 2021 and announced that this would be replaced by a new tool called Topics.

Topics works by using browsing history to determine a number of subjects someone is likely to be interested in.[16] These are kept for a period of three weeks, and shared with participating sites and their advertising partners to use as a basis for targeting. Users can view the topics they have been assigned and are able to delete any of these if they desire.

Topics is still a work in progress and there is the potential for it to follow FLoC in finding little support outside of Chrome and the Google ecosystem. Interestingly, while it appears as a way to target users with relevant ads while maintaining their privacy, Google is set to allow users to opt out of this entirely if they wish. Nevertheless, the company has positioned this as a more trustworthy alternative to cookie-based

advertising, and a preferable option to other methods that could potentially fill the void, such as fingerprinting.

Fingerprinting

Fingerprinting describes a collection of techniques that can be used to identify individuals from information they may not be aware they are sharing through their browsers. It exploits the small differences between different computers or mobile devices, which can include a user's browser, hardware, operating system, time zone, network, cookie settings, and even the fonts they have enabled.

The more information that is available, and the more that this differs from a default configuration, the higher the chance of being able to identify an individual – and with it, the ability to track them across sites. It has been estimated that aprooximately 80-90% of fingerprints are unique,[17] so the appeal of collating this kind of information in order to identify and track individuals is obvious.

What's particularly concerning about fingerprinting is that it's considerably more invasive than cookie-based tracking. While there are legitimate reasons for employing fingerprinting – fraud detection, for example – the average user is unlikely to be aware of the extent of information that is being collected from their online activities, as well as exactly who is collecting this and for what purpose.

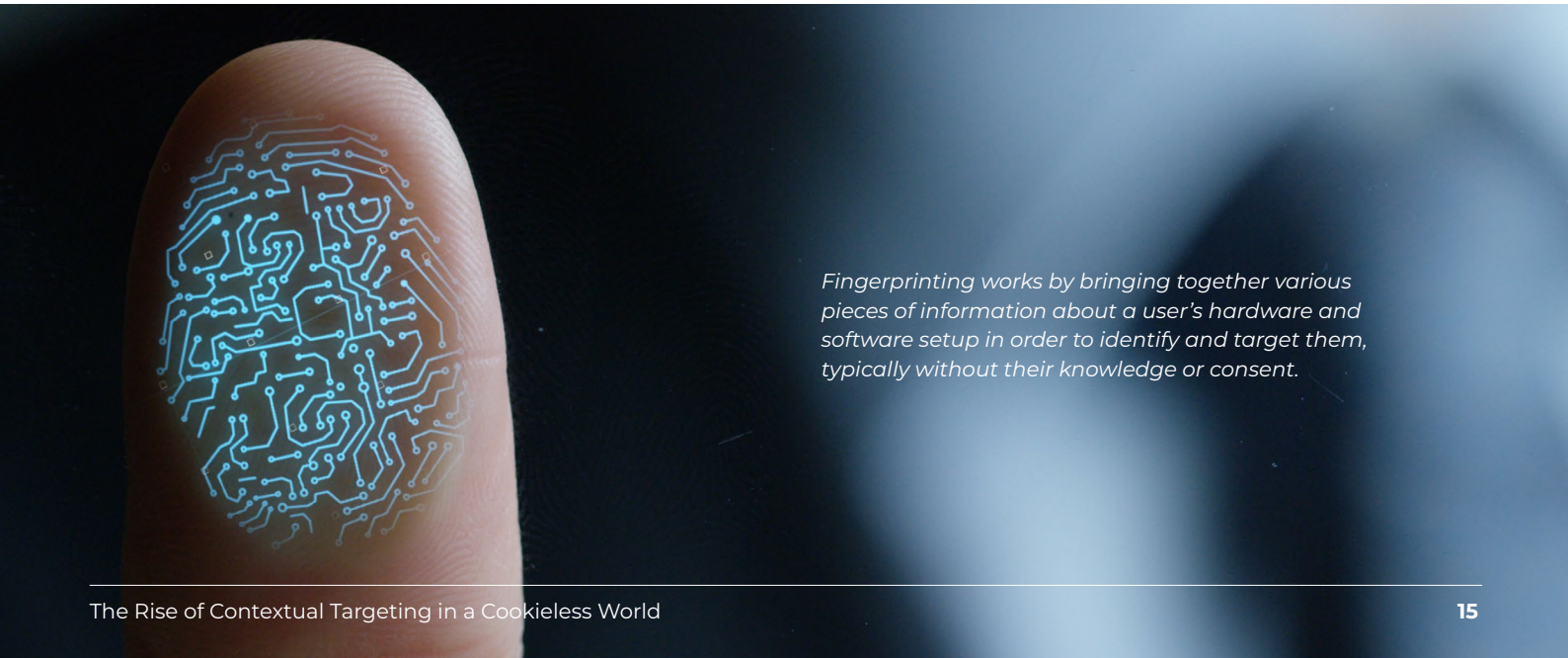
For that reason, it's easy to abuse, particularly when this information is matched with data obtained by other means that can reveal even more about a particular user. And its use is widespread too; in 2020, research showed that 10% of websites in Alexa's top 100,000 websites employed fingerprinting, a figure that rose to 25% when the top 10,000 sites were analyzed.[18]

The future of fingerprinting is somewhat unclear. While it's not as widely understood by the average user as third-party cookies, the threats it poses has been understood for some time by more tech-savvy users and browser providers. As a result, various browser extensions have been developed to help combat this, and many browsers now have some kind of option built in to help defeat this too. The effectiveness of these varies, however, and the reliance of some of these on lists of known fingerprint-collecting sites leaves open the chance of others slipping through the net.

Better first-party data collection

Just as not all fingerprinting is used for nefarious purposes, not all cookies are designed to support questionable practices.

First-party cookies are required by websites to improve user experience, such as by remembering a user's language preferences, login details, shopping cart items, and so on. While they are still used to track behavior, this first-party data is not typically shared with third



Fingerprinting works by bringing together various pieces of information about a user's hardware and software setup in order to identify and target them, typically without their knowledge or consent.

parties, and so it does not facilitate cross-site tracking. As a result, these cookies are enabled at default and are typically kept on by users – and regulations such as GDPR allow this.

Despite not being as intrusive as third-party cookies, however, first-party cookies are not simply there for the user's convenience. Outside of enabling a user to navigate a website with as little friction as possible, they are typically also used by website operators to deliver a highly personalized experience.

For example, a website may use this data to promote products that users are likely to be interested in based on their browsing or purchasing history, or to facilitate a sale by emailing a user to remind them that they left a product in their shopping basket.

Of course, knowing a website's audience, and what an individual's specific interests, habits, and preferences are, can be leveraged for a number of reasons that may not bother the average user. And this helps to explain why the idea of developing this data, and exploring ways of obtaining greater value from it, is one that has gained traction as third-party cookies have started to be phased out.

A repeat visitor to a website is likely to develop a positive impression of it, and might be comfortable volunteering certain information that results in a more relevant experience, be it on the website itself or elsewhere such as via email. If a website operator takes the right steps to build this trust, and solicits details that users may be willing to share, they may find this to be a valuable way to retain their audience's loyalty and simultaneously meet commercial objectives.

Universal IDs

One issue with third-party cookies is the fact that different ad tech companies cannot read each other's cookies. One ad company may assign a user a unique ID under which to store the information they collect about them, and another may do the same under a different ID.

The principle of cookie syncing aims to identify a match and share information with different parties in the ad tech system in order to establish a better idea of who that person is. With better information, advertisers can use this to inform their targeting for greater effect and a better ROI. The more information you have about a user, the better informed you are when it comes to determining whether or not to bid for their attention. This syncing, however, consumes bandwidth and can compromise page load speeds and the overall user experience. Users' details can also be lost in the syncing process.

Universal IDs address these issues. While there are a number of these IDs currently vying for widespread adoption, the idea behind them is that the process of logging into a website with an identifier – typically an email address, but potentially a phone number – creates a standardized, anonymized ID token. To increase privacy, this identifier is hashed and encrypted, with arbitrary information added during the hashing stage – a process known as salting – and the ID is refreshed over time as an additional security measure. Once set, it can be shared with trusted third parties, who can decide which audiences to target.

As a user is assigned a specific identifier linked to their email address, Universal IDs can be used to sync across different browsers and devices that may not normally be talking to one another. Proponents also say that it should make it easier for companies other than Google and Facebook – who together account for just over half of the global ad market spend[19] – to access high-quality targeting data.

However, on top of the uncertainty around which specific Universal ID(s) will end up being adopted, questions remain on how effective this will be if a user does not consent to it – a key requirement for it to work.

Furthermore, the fact that these work on the principle of cross-site tracking, and the potential inclusion of probabilistic data in some of these IDs (such as fingerprinting), also concerns some. The likelihood of Google not supporting these may also be key in determining whether they gain traction and become standard.

6.

The attention economy

As we've started to move into the next evolution of digital advertising, the importance of metrics that are typically used to measure performance – cost per mile (CPM), click-through ratio (CTR), impressions, and so on – has started to be questioned. While these clearly have utility and are unlikely to be abandoned, marketers and advertisers are increasingly looking beyond this to the idea of measuring attention.

The attention economy is built on the premise that attention is a scarce resource. As advertising can only be effective if it is noticed to some degree by its audience, it follows that understanding the ways in which different ad formats, placements, and other variables affect attention can help to determine which kinds of campaigns are likely to be most effective.

When you consider the ever-increasing number of channels and range of devices in which ads are served, and the array of visual, aural, and audio-visual formats that advertisers now have to choose from, it's easy to understand why this information is more valuable than ever before. But part of the appeal of understanding attention can also be attributed to the shortcomings of existing metrics. For example, we may be able to determine that an ad is more viewable, or be gaining more impressions, than another, but this doesn't necessarily mean that it is getting more attention because of it.

One key difference between conventional performance metrics and the measurement of attention is that the latter is measured qualitatively, rather than quantitatively. This means that data on attention cannot be gathered on demand in the same way as it can with clicks and impressions. Most of the studies done on measuring attention with respect to advertising have concerned eye tracking in controlled conditions. Some studies have used front-facing cameras in mobile devices,[20] although quite how easily this could be expanded to work on genuine ads in real-world environments while respecting user privacy is unclear.

Nevertheless, it seems very likely that this will be an area that continues to attract interest. As we gain a greater understanding of the variables that make the greatest difference to ad performance, we should expect new ad formats to be adopted and older ones to be abandoned, particularly on mobile devices, which today account for more internet traffic than desktop devices.[21]

7.

Market forecast

As we have seen, there are many different proposals for the replacement of third-party cookies. But the contextual advertising market is still expected to see significant growth across various territories over the next few years.

One recent study published by Global Industry Analysts estimated that the global market for contextual advertising would be worth $199.8bn in 2022. By 2026, however, the market as a whole is expected to be worth $335.1bn, growing at a CAGR of 13.3% over that period.[22]

When viewed in the context of the global digital advertising and marketing industry, which was estimated to be worth $350bn in 2020 and projected to reach $786.2bn in 2026,[23] contextual advertising is on track to become a dominant component of the advertising mix.

Currently, the US accounts for just under a third of global contextual ad spend at $64.6bn,[24] which itself represents a 13% increase from 2021, when it was valued at $57.1bn.[25] The aforementioned study also predicted that China should grow at a CAGR of 16.3% by the year 2026, while Germany is expected to grow at 12.4%, Japan at 11.3%, and Canada at 11.8%.[26]

It's entirely likely that other territories will eclipse these figures over the next few years, notably India. With a population of 1.38 billion – including over 744 million smartphone users[27] – the country is said to not only have the fastest-growing internet advertising market in the world, but also the fastest-growing mobile ad market, where attention is increasingly being focused. PwC has predicted the online advertising market in India as a whole would grow at a CAGR of 18.8% between 2020-2025, so contextual targeting may well play a significant role in this.[28]

Russia was also pegged as one of the fastest-growing markets at the start of the year, and was expected to show a growth of 11.2% in 2022 over the previous year,[29] although this is likely to be revised following the invasion of Ukraine and the subsequent effect on the country's economy.

8.

Summary

The next few years stand to have a significant effect on the future of online advertising. The introduction of various privacy-focused regulations around the world means that it's highly unlikely that the shift from cookie-based targeting is anything but permanent, and as new regulations continue to be passed in various territories, the global advertising industry will need to remain agile if it's to continue to serve relevant advertising in permissible ways.

What specific mix of ad tech systems will form the backbone of online advertising in the future? Perhaps it's too early to say. Exactly how Google will develop its Topics system; whether this will be adopted more widely by others; and whether one or more Universal IDs will become standard are just three of many unknowns. Also important is the fact that cookie-based targeting may be disappearing, but much of what is being proposed to take its place is still based on behavioral targeting, albeit in a less intrusive form. So the question of how this will be received by online users remains.

Advertising of some sort is essential to the continued operation of many online properties, and many people no doubt appreciate this. So efforts to raise awareness of a value exchange can hopefully lead to a solution that everyone can agree with. This is important, as it's only by taking the needs of all stakeholders into consideration can we build systems that are likely to succeed.

But if we assume that the findings from research into contextual targeting reflect the views of broader audiences, it's reasonable to predict that enough weight will be thrown behind it for it to grow into a dominant targeting format in the years to come.

Sources

1. *Global Contextual Advertising Industry.* Report Linker. Accessed March 2022. Link

2. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Pew Research Center, Accessed February 2022. Link

3. *Amazon hit with $886m fine for alleged data law breach*. BBC. Accessed March 2022. Link

4. *Meta Slapped With $19 Million Fine for EU Data Law Breaches.* Bloomberg. Accessed March 2022. Link

5. *French regulator issues record fines for Facebook and Google cookie violations*. Lexology. Accessed March 2022. Link

6. *What are the GDPR consent requirements?* GDRP EU. Accessed March 2022. Link

7. *GDPR fines: where will BA and Marriott's £300m go?* Accessed January 2022. Link

8. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.* Pew Research Center. Accessed March 2022. Link

9. *The IAB Europe Guide To Contextual Advertising.* The IAB. Accessed March 2022. Link

10. *Importance of Contextual.* The IAB. Accessed February 2022. Link

11. *Importance of Contextual.* The IAB. Accessed February 2022. Link

12. *Everything in context – study reveals power of content-relevant ads.* Warc. Accessed March 2022. Link

13. *Global market share held by leading desktop internet browsers from January 2015 to December 2021.* Statista. Accessed March 2022. Link

14. *Protecting your privacy online.* Google. Accessed March 2022. Link

15. *DuckDuckGo, Firefox & GitHub say 'no FLoCing way' to Google's privacy updates.* The Drum. Accessed March 2022. Link

16. *Get to know the new Topics API for Privacy Sandbox.* Google. Accessed March 2022. Link

17. *The Quiet Way Advertisers Are Tracking Your Browsing*. The Wired. Accessed March 2022. Link

18. *A quarter of the Alexa Top 10K websites are using browser fingerprinting scripts.* ZDNet. Accessed January 2022. Link

19. *Duopoly still rules the global digital ad market, but Alibaba and Amazon are on the prowl.* EMarketer. Accessed March 2022. Link

20. *Are you doing eye-tracking on phones? Here's what you're doing wrong.* Neurons. Accessed 2022. Link

21. *Percentage of mobile device website traffic worldwide from 1st quarter 2015 to 4th quarter 2021.* Statista. Accessed January 2022. Link

22. *Contextual Advertising World Market Report.* StratergyR. Accessed March 2022. Link

23. *Global Contextual Advertising Industry.* Report Linker. Accessed March 2022. Link

24. *Contextual Advertising World Market Report.* StratergyR. Accessed March 2022. Link

25. *Global Contextual Advertising Industry.* Report Linker. Accessed March 2022. Link

26. *Global Contextual Advertising Industry.* Report Linker. Accessed March 2022. Link

27. *Number of mobile phone internet users in India from 2010 to 2020, with estimates until 2040.* Statista. Accessed March 2022. *Link*

28. *India edition: Entertainment & Media Outlook 2021-2025.* PwC. Accessed March 2022. Link

29. *Global Ad Spend Forecasts January 2022.* Dentsu. Accessed March 2022. Link

SMARTFRAME

About us

Founded in 2015, SmartFrame Technologies is a London-based software provider that's redefining the digital image standard. Its SmartFrame platform allows content owners and brands to protect their assets and present them in the best possible way, while also allowing publishers to source and embed high-quality images, and for everyone involved to generate new revenue streams by way of in-image advertising.

Contact us

To find out more about contextual targeting, get in touch with us today.

hello@smartframe.io
smartframe.io