



Journal of Consumer Behavior, Marketing, and Management (JCBMM)

VOLUME 1 ISSUE 1 (2025)



PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

Cookie-Less Advertising and the Future of Customer Targeting in a Privacy-First Era

T. D. Adesina^{1*}

Article Information

Received: May 06, 2025

Accepted: June 11, 2025

Published: August 30, 2025

Keywords

Consumer Trust, Contextual Targeting, Cookie-Less Advertising, First-party Data, Privacy Regulations

ABSTRACT

Cookies are being phased out and create issue with targeting precision, ad efficiency, and ROI as they have traditionally enabled advertisers to follow user activity across sites. This paper explores the impact of a cookie-less future on digital advertising, focusing on developing strategies and technologies designed to allow for effective targeting while adhering to privacy regulations. Major findings show the ascendancy of first-party data as a prized asset for advertisers. In contrast, first-party data is more accurate and collected directly from consumers, which means it is also more privacy compliant than third-party data. First-party data also has its challenges when leveraged at scale, namely the kind of tracking and personalization cookies offered. As a more privacy-friendly practice, interest-based advertising has been replaced or supplemented by contextual advertising, which makes advertising targets according to the content of the website rather than the behaviour of the user. But it is not as accurate as the cookie-based ones. Identity resolution technologies are also under consideration as they allow cross-platform tracking and although they remain compliant with privacy laws, are criticized for their centralization of data and potential for misuse. Consumer trust has required transparency with regards to data collection and consent. Despite the obvious advantages it also raises ethical questions of data abuse that need to be balanced carefully between privacy and personalization. The cookie-less future will not only mean challenges but will be an opportunity for advertising as well. Adopters must bring privacy to the forefront by adopting first-party data and privacy-respecting technologies such as AI personalization, and context-based targeting technologies. Such a scenario will depend on transparency and trust from consumers in such advertising.

INTRODUCTION

Cookies have been the dominant tool for targeting clients in traditional marketing, especially online marketing, as (Shetty, 2022). Cookies, which are small data files that stay on users' browsers, tracked consumer behaviour across sites allowing for profiling and personal ads (Porcelli *et al.*, 2024). These cookies enabled essentially retargeting – displaying ads to users based upon their previous browsing behaviour – as well as cross-site attribution, allowing advertisers to assess the effectiveness of their ads. But cookies have come under fire for consumer about privacy and awareness of data collection, leading to a growing concern over data collection by companies.

The new concern with data protection gave rise to strict privacy legislations such as the European Union's General Data Protection Regulation Act (GDPR) and the California Consumer Privacy Act (CCPA) in the U.S (Farhad, 2024). These models aim to give individuals rights over their own data and to create responsibilities for companies to collect and use personal data (Morić *et al.*, 2024). This has led to a reassessment at how businesses will transition into marketing in a privacy-centric world, and trust and data protection have become the new branding and advertising paradigms.

These privacy concerns have resulted in the death of third-party cookies and as a result cookie-less advertising. This was the trade off the industry offered in terms of

targeting versus consumer privacy deference. Advertisers adapted by using first-party data, contextual ads, and privacy-protecting technologies among other measures to fill the need for tracking users through cookies in a world without them (Morić *et al.*, 2024).

The other important benefit is first-party data, which is information acquired from customers, and with their consent. The scaling issues are the same as first-party data and provenance and permission are still a challenge. Also, there is contextual targeting – ads are placed according to the content of a web page rather than according to users' previous behaviours – but this is much less accurate than cookie-based targeting. These are fundamentally creative problems, and a transition to privacy-protecting advertising technologies that are capable of delivering such personalized advertisements without invading people's privacy. The purpose of this paper is to understand the impact of a cookie-less future on targeted advertising.

LITERATURE REVIEW

Cookies have long served as a means through which advertisers can monitor and track users across websites. This enables them to deliver more tailored ads by developing profiles of users based on their website visits, searches, and purchases, even beyond the site the user is currently visiting. These profiles allow better precision in targeting ads, ads that become relevant for the users'

¹ Trocah Technology Limited, 128 City Road, London, EC1V 2NX, United Kingdom

* Corresponding author's e-mail: adesina.damilola@trocah.com

interests and needs, thus increasing effectiveness and ROI of advertising. (Ullah *et al.*, 2022; Sim *et al.*, 2024). Cookie-based advertising methods started to be defined in the late 1990s, when cookies were created to store user preferences and manage sessions. Cookies eventually became capable not only of facilitating targeted advertising, but also retargeting, or showing ads to users for products they had viewed or interacted with previously (Hana *et al.*, 2022). The strength of this kind of remarketing was a large part of the cookie-based strategies' effectiveness, in that, it continued to make relevant ads visible to consumers as they navigated the web.

As cited by Leguina *et al.* (2020), cookies allowed for cross-site attributes, providing information to evaluate the effectiveness of advertisements across multiple sites. As a result, more intelligent decisions regarding advertising expenditures were done because tracking conversions among multiple sites was possible. Cookies, on the one hand, are helpful and more efficient, for personalized ads creation, but on the other hand, they have been accused of privacy and data security problems. As a consequence, the advertising industry is moving toward privacy-centric alternatives that remain efficacious (Abdallah *et al.*, 2025; Alkis & Kose, 2022; Miller & Skiera, 2023; Strycharz *et al.*, 2021).

The Rise of Privacy Regulations

Perhaps the most well-known regulatory answer of this type is the General Data Protection Regulation, or GDPR, which relates to consumer privacy and has been in effect in the European Union since 2018 (Ebrahimi *et al.*, 2022; (Hoofnagle *et al.*, 2019). GDPR enforces strict responsibilities on companies with regards to collecting, storing and processing personal data, while empowering consumers with their data. Similarly, the California Consumer Privacy Act (CCPA) or California Consumer Privacy Act, enacted in 2020, allows consumers to “opt out of the sale of that person’s personal information” and obliges companies to notify consumers about their collection of personal data (Baik, 2020). This has had a particularly strong impact on digital advertising and has led advertisers to rethink their use of consumer data. This requirement for active consent is why cookie-based tracking methods are no longer in use.

With increased consumer desire for more ethical and transparent advertising arises more regulatory interest. According to some study, more consumers than ever before are concerned about privacy and the use of their personal information for marketing purposes. These shifts in consumer mindset have pushed organizations to adhere to privacy laws and implement a customer-centric trust-first ethical advertising technique (Adanigbo, 2024; Chavan & Lima, 2024; Dwivedi *et al.*, 2020; Hemker *et al.*, 2021; Rosário & Dias, 2023).

Cookie-Less Advertising: Emerging Trends and Technologies

As the industry transitions to a future without cookies, numerous innovative strategies have started to address

the tracking capabilities previously provided by third-party cookies. A key solution is the heightened utilization of first-party data, which refers to information gathered directly from consumers during their interactions with a brand’s website or application (Dwivedi *et al.*, 2020). First-party data is also more precise than third-party data, and it adheres to legal standards since it is collected with the consent of users and shared voluntarily. This type of data enables advertisers to customize experiences for individuals while respecting consumer privacy.

Another viable cookie-free solution which places ads according to the content of a website other than the consumer behaviour is “Contextual advertising” (Hana *et al.*, 2022). It is a privacy-preserving alternative because it is not based on user tracking across multiple sites. Advertisers may offer relevant ads without breaching anyone’s privacy by examining the context of the page, i.e., through keywords or themes of content. Also rising in popularity is server-side tracking, or tracking that occurs and is managed on the server rather than on the client. Interestingly, this methodology allows advertisers to further improve how ads are targeted while also collecting data in a more privacy-preserving manner.

Unified IDs are yet another rising option in the cookie-less advertising world (Shetty, 2022, 2022). These IDs are unified identifiers that amalgamate multiple pieces of data from different platforms into one ID for a given user, allowing advertisers to follow the user across all platforms but “in a privacy-compliant way”. The problem with unified IDs, but, is the centralization of data and the risk of abuse of it.

New alternatives, such as browser fingerprinting, device IDs and local storage, are also being considered for cross-site user tracking (Pau *et al.*, 2023). Although, these methods provide new ways to collect data, they also raise privacy concerns. Browser fingerprinting, for example, identifies users by their unique browser characteristics, but it does so without user consent, which further leads to potential ethical and legal issues.

Consumer Perceptions of Privacy in Advertising

Privacy perception by consumers is therefore key to the efficacy of cookie-less advertising techniques. In light of this awareness, trust has been implicated in consumer attitudes in relation to data. Consumers have been found to be sceptical regarding the use of their personal data and privacy is reportedly among the foremost digital content and advertising concerns (Cai & Mardani, 2023; Ho *et al.*, 2023; Quachet *et al.*, 2022; Yadav *et al.*, 2024).

The cookie-less change is both challenging and providing a means to build a good relationship with consumers. Trust relies heavily on transparency regarding data collection practices. Consumers prefer brands that are transparent of the usage of their information and provide clear opt-in preferences for data collection. Consumers would feel greater engagement and trust as they would control their data and be using privacy advertising responsibly (Adanigbo, 2024).

Data protection is also a key factor in framing consumer behaviour. Those that protect data and give control to consumers over their own information are more likely to foster consumer loyalty in the long run. Still, those that do not provide transparency or apply unethical data practices will further face challenges of consumer trust which will translate in effectiveness of advertising and or in maintaining customers (Sansome *et al.*, 2023).

In this present privacy-centric generation of advertising, trust and the ability to defend privacy will oversee. Brands are beginning to see that privacy-focused techniques are the future of advertising, and as a result, they must establish more ethical and sustainable strategies.

MATERIALS AND METHODS

This study employs a qualitative secondary research approach, drawing on a total of 30 secondary sources to explore the implications of a cookie-less digital advertising environment. The dataset includes 12 peer-reviewed journal articles, 10 industry reports and white papers, and 8 regulatory and policy documents. To ensure relevance and credibility, the selection process followed specific inclusion and exclusion criteria. Sources were included if they were published between 2018 and 2025, addressed themes such as digital advertising, customer targeting, data privacy, or regulatory impacts, and originated from reputable academic, industry, or governmental platforms. Searches were conducted using databases such as Google Scholar, Scopus, and industry sources like IAB Europe, Deloitte Insights, and McKinsey, alongside regulatory sites including the official EU GDPR and CCPA portals. Opinion-based articles, blog posts without data citations, and materials predating 2018 were excluded unless they were deemed foundational to the topic. This structured approach ensured that the analysis was based on a balanced, current, and authoritative body of evidence. Through an emphasis on multiple forms of tracking, it explains the ways in which privacy laws like the CCPA and GDPR are affecting the shifts in advertising methods and the ways companies are adjusting their methods to resolve the drawbacks of reduced cookie use. The analysis summarizes the topmost techniques and forecasts future trends in digital marketing and privacy- respecting client targeting.

RESULTS AND DISCUSSION

Among the findings is a conclusion that first-party data are now a core asset for advertisers. While third-party cookies were based on data from outside sources, first-party data comes from users' direct interactions with a brand's website or app. Amongst other details, this data comprises users' website browsing behaviours, previous purchases, and preferences, which can be used to personalize advertising in a privacy-compliant way (Dwivedi *et al.*, 2020). In fact, this move toward first-party data has been seen as a good thing, in that it enables advertisers to create customized experiences from consumer permission and interaction. The problem with

first-party data at scale, but, is that it is highly accurate, but also limited. Though third-party data was particularly valuable in developing comprehensive consumer profiles, it has now largely disappeared and has been subject to a disconnect between "consent, transparency, and commodification of personal information" (Sim *et al.*, 2024; Shetty, 2022). Nonetheless, firms such as Amazon and Apple have been able to use first-party data to provide very personalized advertisements while also complying with privacy policies. Interestingly, it quickly revealed that businesses could successfully serve personalized advertising in a post-cookies world, provided they had certain technologies and techniques, such as using integrated customer data platforms. But advertisers will though have to learn how to collect and manage large amounts of first-party data while avoiding user privacy concerns or opt-in fatigue (Ebrahimi *et al.*, 2022).

The reduced targeting precision which has been inculcated in Cookieless advertising as generally affected the measurement of ad effectiveness and cross-platform tracking. Most time, when there are no cookies, advertisers struggle to obtain direct information about ad performance metrics from user journeys. Cookie-based attribution is being replaced by methods like Media Mix Modelling (MMM) analysis and incrementality testing. MMM usually examine past sales records and media expenditures in various channels to evaluate the success of marketing campaigns and assist advertisers to understand how various marketing activities connect with the overall return on investment or ROI from marketing expenditures (Einhorn, 2025).

Also, incrementality testing is where different advertising approaches are tried out to obtain data on the actual effects of advertising on consumer behaviour. These approaches can be useful, but they lack the level of precision that cookies can provide, especially at the individual level (Sim *et al.*, 2024). But, in a context where advertisers need more than ever to achieve the highest possible ROI, adding AI-based analytics will definitely become necessary to cover what these tools will start to miss out due to the lack of cookies.

This has limited the potential to maximize return on investment. Replacing third-party cookies is about shifting from an advertising model based on opaque data collection and targeting to one centred on fielding transparent data and consent to target, but whose implementation may not be as easily deployed and may demand more

work and costs. Still, first-party data's advantages, such as enhanced consumer relationships and greater data accuracy, are now being understood as critical to continuing to have effective advertising in this new context.

The elimination of this has been documented to have significant impact for marketers, in that they lose the capacity to track consumer behaviour across external sites. But, without cookies, the ability to monitor users' movement across websites and devices has been complicated, which limited advertisers' ability to access

cross-platform attribution data (Sim *et al.*, 2024). Advertisers are beginning to address this gap in several ways. Hana *et al.* (2022) Server-side tracking presents companies with the ability to track users on the server instead of through the now-limited browser tracking that can no longer be relied upon. According to Hana *et al.* (2022), server-side tracking

Alternative Advertising Strategies and Technologies

The advertising industry has accordingly started to use a set of other technologies and practices in response to the “death of cookies,” which would provide for effective targeting within the limits of privacy. As an alternative to behavioural targeting, contextual targeting has become a more common practice. Contextual advertising displays ads based on the content of a webpage rather than using information from users.

A newer solution is identity resolution. It gathers data at different touchpoints and builds a sort of identity profile on that specific consumer, often via merge or known ID. Privacy-compliant unified ID solutions link the activity of a user across platforms. This reduces the reliance on third-party cookies and allows advertisers to maintain their capacity to target ads cross-platform. Identity resolution can be effective as mentioned, but it does involve an exact dosage of personalization and privacy safeguarding because consent is key in the data collection process.

Artificial Intelligent (AI) based personalization, plus, has begun to look appealing as a new alternative. Without the use of cookies, AI and Machine Learning (ML) techniques can allow advertisers to display targeted ads. These technologies can parse consumer behaviour, interests, and demographic information to serve more contextual and relevant ads. AI solutions can achieve the same level of cookie-based precision, but in a real-time context that respects privacy laws.

There has also been mention of the role of Consent Management Platforms (CMPs) and data clean rooms. CMPs allow advertisers to gather data in a privacy compliant manner; consumers have control over their data but businesses can still gain valuable insights. Data clean rooms, in contrast, enable brands to process first-party data in a private way. Both technologies give advertisers the ability to use data to drive decisions without putting consumer data at risk.

Consumer Trust and Ethical Perceptions in Cookie-less Advertising

Considering Cookieless future, customer trust will be very important to advertisers. Moving to privacy-first advertising methods has significantly impacted and improved consumers’ understanding of brand relationships. This is because, when consumers can control the manner in which their data is collected and are educated regarding the ways in which it is used, they are quick to trust businesses. Transparency of the data collection process is one of the major reasons fostering this kind of confidence. When privacy is valued and information is treated ethically, consumers are more willing

to engage with ads and provide accurate information.

The ethical issues of cookie-less advertising are still considerable though. An overarching concern is of course the abuse of personal data. As exposed to the potential exploitation of their personal data, consumers are becoming more aware of the ways in which their information can be used to target them with advertisements and are thus beginning to demand transparency and permission-based approaches that incorporate consumer consent to data collection. Nonetheless, the advanced methods of data collection and the potential abuses in a society without cookies still looms as a serious ethical problem.

Comparing Traditional and Cookie-less Advertising

Both cookie-based advertising and cookie-less advertising come with their own advantages and drawbacks. Cookie-based advertising in the old sense accepted behaviour tracking across sites, and led to good targeting, retargeting, and attribution. It allowed for very specific advertising and more efficient use of advertising dollars as it detailed each individual consumer’s behaviour. It also created one of the biggest issues on privacy, in that most users were unaware of the amount of data being tracked and the nature of the profiles.

Cookie-less advertising, on the other hand, emphasizes privacy-friendly data, such as first-party data and contextual targeting. These are more ethical forms of advertising, but they don’t have the same granularity or real-time tracking capabilities that cookies did. But now AI-powered personalization and identity resolution technologies are filling that void – enabling relevant, personalized experiences without the use of cookies.

At the end of the day, cookie-less alternatives won’t achieve the same type of accuracy that cookie-based methods can provide, but they can be a way to develop personalized ads without violating consumer privacy. Advertisers need to accept these new technological changes, impact and challenges, commit to openness and transparency, and work to develop relationships of trust with consumers in order to successfully make the shift towards a privacy-first advertising future.

Implications for the Future of Advertising

The death of cookies is already affecting ad spend, consumer engagement and branding. Given that third-party cookies are no longer an option, advertisers will need to be looking for new ways to track shifts to more private alternatives like first-party data and contextual targeting. Adopters and/or those interested in making the transition will likely face higher advertising costs but, as they will need to invest in and learn to use technologies and tools like Consent Management Platforms (CMPs), data clean rooms, and identity resolution to continue to appropriately target customers while adhering to privacy regulations.

The ability to track performance in such detail will be lost, and during a period of time, until brands learn to do it differently, the performance of advertising could decrease. But the key will be to adjust to a privacy-first

marketing ecosystem and those that can do it successfully will win in the long term. Brands will have to focus on being trustworthy and providing transparent data practices. This trend toward more privacy-oriented advertising could open a door to include customer interaction via first-party data and bolstering those relationships. Moving forward, brands will have to think of this industry with data and ethics in mind, focusing on consent and security of data.

The Role of Privacy Regulations in Shaping Future Advertising

These laws will not only affect the EU and California, as digital marketing is globalized and, in the future, laws will probably have to be harmonized. There is also the possibility that this would mean the adoption of global privacy legislations, which would change advertising everywhere. Balancing the understanding of effective targeting and measurement as well as dealing with the challenges of multiple regulatory frameworks will be a challenge for advertisers. As regulation increases, companies will have to embrace privacy enhancing technologies and focus on data reduction to minimize the amount of personal data they collect. In the long run, these rules should eventually encourage responsible and transparent marketing practices that build consumer trust and brand equity. Brands that embrace these changes will ensure compliance, but more importantly will gain a competitive advantage.

CONCLUSION

This paper has looked at the impact of cookie-less advertising on how customers are targeted, focusing on the shift to privacy-first marketing and the new replacements for traditional cookie-based methods. The findings indicate that as third-party cookies are being suppressed in response to mounting privacy concerns and data protection measures, the advertising industry has increasingly begun to rely on first-party data and contextual targeting. These provide a solution to continue supplying personalized advertising and to do so at the expense of consumer privacy. There are downsides to the shift but, particularly around the ability to maintain ad performance and returns on investment. While advertisers and businesses are learning to adjust to privacy-centric methods such as identity resolution, AI personalization, and CMPs, the effectiveness of these novel methods is still evolving. This is an ethical matter. This shift towards privacy-first advertising has led an increased transparency on the process of collecting and utilizing consumer data, further enhancing consumers' trust. Still, the misuse of personal data and questions about "ethical opt-in" models, among other issues, remains problematic. The cookie-free future has both challenges and possibilities. Just as privacy rules increase, the advertising industry will need to incorporate technologies that combine advertising productivity with privacy compliance, establishing companies as responsible and trustworthy organizations in the eyes of consumers.

Recommendations

It is clear from this study, that the advertising industry is undergoing a major shift in response to increasing privacy regulations and the deprecation of third-party cookies. Therefore, the following recommendations are made for businesses undergoing this transition:

1. Advertisers should stick to the collection and the use of first-party data, which is gathered directly from users with their approval. Although, it may not give the same depth of information as third-party cookies, it supports privacy compliance and is more accurate.
2. Using of technologies like; contextual advertising, AI-driven personalization, and identity resolution can assist in maintaining targeted advertising without compromising privacy.
3. To remain in compliance with privacy regulations including the GDPR and CCPA, businesses should make sure that they implement CMPs which give consumers control over their data and ensure transparency in data collection practices.
4. Finally, brands should explicitly state, convey their data collection procedures, and guarantee consumers consent to data use as this will improve customer trust and brand reputation.

REFERENCES

- Abdallah, A., Ahmad, A., & Said, B. (2025). Balancing Privacy and Usability: A design science research approach for cookie consent mechanisms. *Journal of Open Innovation Technology Market and Complexity*, 100520. <https://doi.org/10.1016/j.joitmc.2025.100520>
- Adanigbo, O. S. (2024). Consumer privacy concerns in digital marketing: A review paper. *IRE Journals*, 8(2), 469.
- Alharbi, J. A., Albeshier, A. S., & Wahsheh, H. A. (2023). An empirical analysis of E-Governments' cookie interfaces in 50 countries. *Sustainability*, 15(2), 1231. <https://doi.org/10.3390/su15021231>
- Alkis, A., & Kose, T. (2022). Privacy concerns in consumer E-commerce activities and response to social media advertising: Empirical evidence from Europe. *Computers in Human Behaviour*, 137, 107412. <https://doi.org/10.1016/j.chb.2022.107412>
- Baik, J. (2020). Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). *Telematics and Informatics*, 52, 101431. <https://doi.org/10.1016/j.tele.2020.101431>
- Cai, H., & Mardani, A. (2023). Research on the impact of consumer privacy and intelligent personalization technology on purchase resistance. *Journal of Business Research*, 161, 113811. <https://doi.org/10.1016/j.jbusres.2023.113811>
- Chavan, R., & Lima, M. (2024). Personalization vs. privacy: Consumer attitude towards data collection for marketing. *International Journal of Research Publication and Reviews*, 5(7), 2347–2350. <https://www.ijrpr.com>
- Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., Jain, V., Karjaluoto, H.,

- Kefi, H., Krishen, A. S., Kumar, V., Rahman, M. M., Raman, R., Rauschnabel, P. A., Rowley, J., Salo, J., Tran, G. A., & Wang, Y. (2020). Setting the future of digital and social media marketing research: Perspectives and research propositions. *International Journal of Information Management*, 59, 102168. <https://doi.org/10.1016/j.ijinfomgt.2020.102168>
- Ebrahimi, P., Basirat, M., Yousefi, A., Nekomahmud, M., Gholampour, A., & Fekete-Farkas, M. (2022). Social networks marketing and consumer purchase behaviour: the combination of SEM and unsupervised machine learning approaches. *Big Data and Cognitive Computing*, 6(2), 35. <https://doi.org/10.3390/bdcc6020035>
- Einhorn, T. (2025). *The difference between incrementality, MMM, and MTA*. Measured®. <https://www.measured.com/faq/what-are-the-pros-and-cons-of-incrementality-testing-versus-mmm-or-mta/>
- Farhad, M. A. (2024). Consumer data protection laws and their impact on business models in the tech industry. *Telecommunications Policy*, 48(9), 102836. <https://doi.org/10.1016/j.telpol.2024.102836>
- Hana, N., Guérin, M.-M. and Sabri, O., (2022). *Cookiepocalypse: What are the most effective strategies for advertisers to reshape the future of display advertising?* Published by Elsevier. Available at: <https://www.elsevier.com/open-access/userlicense/1.0/>.
- Hemker, S., Herrando, C., & Constantinides, E. (2021). The Transformation of Data Marketing: How an ethical lens on consumer data collection shapes the future of marketing. *Sustainability*, 13(20), 11208. <https://doi.org/10.3390/su132011208>
- Ho, F. N., Ho-Dac, N., & Huang, J. S. (2023). The effects of privacy and data breaches on consumers' online Self-Disclosure, protection behaviour, and message valence. *SAGE Open*, 13(3). <https://doi.org/10.1177/21582440231181395>
- Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1), 65–98. <https://doi.org/10.1080/13600834.2019.1573501>
- Leguina, J. R., Rumín, Á. C., & Rumín, R. C. (2020). Digital Marketing Attribution: Understanding the user path. *Electronics*, 9(11), 1822. <https://doi.org/10.3390/electronics9111822>
- Miller, K. M., & Skiera, B. (2023). Economic consequences of online tracking restrictions: Evidence from cookies. *International Journal of Research in Marketing*, 41(2), 241–264. <https://doi.org/10.1016/j.ijresmar.2023.10.001>
- Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of personal data in the context of E-Commerce. *Journal of Cybersecurity and Privacy*, 4(3), 731–761. <https://doi.org/10.3390/jcp4030034>
- Pantelic, O., Jovic, K., & Krstovic, S. (2022). Cookies implementation analysis and the impact on user privacy regarding GDPR and CCPA regulations. *Sustainability*, 14(9), 5015. <https://doi.org/10.3390/su14095015>
- Pau, K. N., Lee, V. W. Q., Ooi, S. Y., & Pang, Y. H. (2023). The development of a data collection and browser fingerprinting system. *Sensors*, 23(6), 3087. <https://doi.org/10.3390/s23063087>
- Porcelli, L., Mastroianni, M., Ficco, M., & Palmieri, F. (2024). A User-Centered Privacy Policy management system for automatic consent on cookie banners. *Computers*, 13(2), 43. <https://doi.org/10.3390/computers13020043>
- Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6), 1299–1323. <https://doi.org/10.1007/s11747-022-00845-y>
- Rosário, A. T., & Dias, J. C. (2023). How has data-driven marketing evolved: Challenges and opportunities with emerging technologies. *International Journal of Information Management Data Insights*, 3(2), 100203. <https://doi.org/10.1016/j.ijime.2023.100203>
- Sansome, K., Wilkie, D., & Conduit, J. (2023). Beyond information availability: Specifying the dimensions of consumer perceived brand transparency. *Journal of Business Research*, 170, 114358. <https://doi.org/10.1016/j.jbusres.2023.114358>
- Shetty, A. (2022). The Future of Cookieless Advertising: Adapting to Privacy-Focused Identity Solutions. *Journal of Scientific and Engineering Research*, 9(12), 202–209. Available online: www.jsaer.com.
- Sim, K., Heo, H., & Cho, H. (2024). Combating web tracking: Analyzing web tracking technologies for user privacy. *Future Internet*, 16(10), 363. <https://doi.org/10.3390/fi16100363>
- Strycharz, J., Smit, E., Helberger, N., & Van Noort, G. (2021). No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behaviour*, 120, 106750. <https://doi.org/10.1016/j.chb.2021.106750>
- Ullah, I., Boreli, R., & Kanhere, S. S. (2022). Privacy in targeted advertising on mobile devices: a survey. *International Journal of Information Security*, 22(3), 647–678. <https://doi.org/10.1007/s10207-022-00655-x>
- Yadav, D., Kala, K., Kolachina, R. I. R., Kanneganti, M. C., & Pasupuleti, S. S. (2024). Data Privacy Concerns and their Impact on Consumer Trust in Digital Marketing. <https://www.semanticscholar.org/paper/Data-Privacy-Concerns-and-their-Impact-on-Consumer-Yadav-Kala/693fc22ac2e246dac7d51b62f57b8d60b6a213ba>