Data Protection and Privacy Law in the Context of Digital Advertising and Tracking

1. Clara Hoffmann: Department of International Law, University of Vienna, Vienna, Austria
2. Tobias Meier*: Department of International Law, University of Vienna, Vienna, Austria

***Correspondence: e-mail: MeierTobey10@gmail.com**

Abstract

Digital advertising has become a cornerstone of the modern digital economy, driving significant economic growth and shaping online experiences for consumers. However, this growth comes with increased concerns about data privacy and protection, as sophisticated tracking technologies enable advertisers to collect vast amounts of personal data. This article explores the intersection of data protection laws and digital advertising, focusing on the key privacy risks and legal challenges associated with tracking technologies such as cookies, pixels, and behavioral tracking. It examines the principles of data privacy, including consent, data minimization, and user control, and provides an overview of major legal frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), as well as emerging privacy standards worldwide. The article discusses the privacy concerns and risks inherent in digital advertising, including surveillance, data security, and the lack of consumer control over personal data. It also addresses the tension between privacy and innovation, offering solutions such as privacy-enhancing technologies and contextual advertising models that aim to balance both interests. In addition, the paper presents future directions for the evolution of data protection laws and highlights the role of emerging technologies like artificial intelligence and blockchain in shaping the future of privacy in digital advertising. Finally, the article provides policy recommendations for businesses and regulators to help navigate the evolving privacy landscape while fostering innovation in digital advertising practices. This article contributes to the ongoing debate on how to protect consumers' privacy rights while enabling the growth of the digital advertising industry.

Keywords: Digital advertising, data protection, privacy law, GDPR, tracking technologies, consumer rights.

Received: 07 May 2024
Revised: 18 June 2024
Accepted: 24 June 2024
Published: 01 July 2024

Citation: Hoffmann, C. & Meier. (2024). Data Protection and Privacy Law in the Context of Digital Advertising and Tracking. *Legal Studies in Digital Age*, 3(3), 15-22.

1. Introduction

Digital advertising has become a cornerstone of the modern economy, significantly transforming how businesses engage with consumers. In the past two decades, the digital advertising landscape has evolved from traditional banner ads to sophisticated forms of targeted advertising that leverage vast amounts of personal data. Central to this evolution is the use of digital tracking technologies, which allow advertisers to gather detailed insights into users' online behaviors, preferences, and demographics. Cookies are among the most well-known tracking tools used in digital advertising. These small text files are stored on a user's device when they visit a website, allowing the site to remember certain actions or preferences over time. This

enables advertisers to create personalized ad experiences, serving relevant content based on an individual's browsing history (European Commission, 2021). Alongside cookies, more advanced tracking techniques have emerged, such as behavioral tracking, which monitors and analyzes users' actions across different websites and devices. This allows advertisers to build detailed user profiles that can be used for highly targeted marketing. Data analytics and machine learning algorithms further enhance the precision of these methods, processing enormous datasets to predict future behaviors and optimize ad delivery (Sweeney, 2019).

The rise of digital advertising has prompted growing concerns over the protection of user data and privacy. With the vast quantities of personal information collected through these tracking mechanisms, there is an increasing risk that this data could be misused or exposed. In particular, behavioral tracking and the creation of detailed user profiles raise questions about consent, transparency, and the extent to which individuals are aware of how their data is being used. Consumers often have limited control over their data, as tracking technologies operate seamlessly in the background while users navigate the web. This lack of transparency has led to significant concerns about the erosion of privacy, especially when personal data is shared across multiple platforms without explicit user consent (Tufekci, 2018). The growing prevalence of data breaches and unauthorized data sharing has only heightened these concerns, with sensitive personal information being exposed or sold to third parties for purposes that individuals may not fully understand or agree with. Moreover, as the scope of digital advertising expands, so does the amount of personal information collected, making it increasingly difficult for users to maintain control over their digital identities and online behaviors (Solove, 2021).

Data protection and privacy are of paramount importance in the context of digital advertising and tracking. As more aspects of individuals' lives are reflected in the data they generate online, protecting this information becomes critical to safeguarding their fundamental rights. Privacy is a cornerstone of individual autonomy, and when personal data is collected and used without proper safeguards, it undermines this autonomy and can lead to exploitation. Beyond the ethical implications, the legal landscape surrounding data protection has become more complex, with various regulatory frameworks being introduced to ensure that individuals' rights are respected. Laws such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States have established stricter guidelines for how personal data must be handled, providing individuals with more control over their information and enhancing accountability for organizations that collect and use this data (Regan, 2020). These regulations are designed not only to protect consumers but also to foster trust in digital platforms, which is crucial for the continued growth of the digital advertising industry.

The importance of these privacy protections becomes even more evident when considering the sensitive nature of the data involved. Beyond simple identifiers such as names or email addresses, digital advertising often relies on deeply personal information, including browsing history, online purchase behavior, location data, and even health-related data. When aggregated, this data can create highly accurate and intrusive profiles that may be used for purposes beyond advertising, such as manipulating political opinions or exploiting vulnerable individuals. Given the potential consequences of this data collection and its use, it is essential to have robust legal frameworks that ensure transparency, control, and accountability (Kuner, 2020). Additionally, as technological advances continue to drive new forms of advertising and tracking, it is crucial that privacy laws evolve in tandem to address emerging threats and challenges.

The goal of this article is to explore the intersection of data protection and privacy laws with digital advertising and tracking technologies. Specifically, the article seeks to examine how current legal frameworks, such as the GDPR and CCPA, apply to the digital advertising ecosystem, with a focus on consent mechanisms, transparency, data subject rights, and enforcement. The paper will also discuss the challenges faced by businesses in complying with these regulations, especially in the context of cross-border data flows and the rapid pace of technological innovation in digital advertising. This research aims to provide a comprehensive understanding of the legal landscape surrounding digital advertising and data privacy, highlighting the balance between protecting consumers' rights and allowing businesses to innovate and thrive in a data-driven economy (Greenleaf, 2019).

This article adopts a descriptive analysis methodology, systematically reviewing the existing literature and legal frameworks on data protection, privacy, and digital advertising. By analyzing the practical applications of privacy laws in the digital advertising context, the article will provide insights into how these regulations are shaping the industry and what challenges remain for both regulators and advertisers. In doing so, the article aims to contribute to the ongoing discourse on privacy, data protection, and the evolving relationship between technology and law in the digital age.

2. Conceptual Framework

Digital advertising refers to the use of online platforms and technologies to deliver promotional content to users. This form of advertising has become increasingly sophisticated as advertisers rely on user data to create personalized and targeted ads. The key tools in digital advertising include cookies, which are small text files stored on users' devices when they visit websites. These cookies allow advertisers to track users' browsing behaviors, such as the pages they visit, the products they view, and the time spent on certain sites. This data is used to tailor ads to users' preferences and browsing history. In addition to cookies, pixels, or small snippets of code, are embedded in websites and email marketing content to track user interactions. These pixels gather data on actions like clicking on an ad or completing a purchase, which helps advertisers gauge the effectiveness of their campaigns. Cross-device tracking is another important technique that enables advertisers to follow users across multiple devices, such as smartphones, tablets, and desktop computers. This provides a more holistic view of consumer behavior and allows for more accurate targeting. Together, these technologies enable advertisers to collect extensive data on users, which can then be analyzed using sophisticated algorithms to refine marketing strategies and enhance user targeting (European Commission, 2021).

Privacy and data protection are essential concepts in the digital age, particularly as personal data is increasingly collected, processed, and used for various purposes, including advertising. At the core of privacy is the idea that individuals should have control over their personal information and how it is shared. Data protection, on the other hand, focuses on safeguarding personal data from misuse, unauthorized access, or exposure. One of the fundamental principles of data protection is consent, which requires organizations to obtain explicit permission from individuals before collecting or using their data. This consent must be informed, meaning individuals should understand what data is being collected, for what purpose, and how it will be used. Data minimization is another crucial principle, which dictates that only the minimum amount of personal data necessary for a specific purpose should be collected. This helps reduce the risks associated with data breaches and unauthorized access. Additionally, user control is central to privacy and data protection, empowering individuals to manage their data preferences and exercise their rights, such as the right to access, correct, or delete their data. These principles are intended to strike a balance between the benefits of data-driven advertising and the protection of individual privacy (Regan, 2020).

Several legal frameworks govern data protection and privacy, with the goal of safeguarding individuals' personal information in an increasingly data-driven world. The European Union's General Data Protection Regulation (GDPR) is one of the most comprehensive and influential privacy laws, setting strict standards for the collection, processing, and storage of personal data. It emphasizes principles such as transparency, accountability, and data minimization, requiring organizations to obtain clear consent from individuals before processing their data. Similarly, the California Consumer Privacy Act (CCPA) grants California residents significant control over their personal information, allowing them to request details about the data being collected, opt-out of data sales, and request the deletion of their data. In addition to these region-specific laws, international privacy standards such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data offer guidelines for cross-border data protection, promoting consistent standards for privacy across different jurisdictions. These legal frameworks aim to ensure that individuals' rights are upheld, even as the digital advertising industry continues to expand and evolve (Kuner, 2020).

3. Legal Landscape of Data Protection in Digital Advertising

The General Data Protection Regulation (GDPR), enacted by the European Union in 2018, has had a profound impact on digital advertising and tracking. It sets out stringent requirements for the collection and processing of personal data, and its effects are felt across the digital advertising ecosystem. A central tenet of the GDPR is consent, which must be freely given, specific, informed, and unambiguous. This requirement has reshaped how advertisers collect data, as users must actively opt-in to tracking and data collection, often through cookie banners or privacy settings on websites. Furthermore, the GDPR places a strong emphasis on transparency, mandating that organizations provide clear and accessible information about how personal data is used, which has led to increased disclosure in digital advertising practices. The regulation also grants individuals enhanced rights, including the right to access, rectify, and delete their data, and the right to withdraw consent at any time. These rights give users more control over their data, compelling businesses to adopt more privacy-conscious approaches to digital advertising. In addition to these rights, the GDPR also introduces significant penalties for non-compliance, with fines reaching

up to 4% of a company's annual global revenue, underscoring the importance of adhering to the regulation. As a result, the GDPR has forced advertisers to rethink their data collection and processing strategies, balancing personalized advertising with user privacy (European Commission, 2021).

The California Consumer Privacy Act (CCPA), enacted in 2020, has introduced similar privacy protections for residents of California, making it one of the most important privacy laws in the United States. The CCPA provides individuals with the right to know what personal data is being collected, the right to opt-out of the sale of their data, and the right to request the deletion of their data. One of the key provisions of the CCPA is its applicability to a wide range of businesses, including those that collect personal data for digital advertising purposes. The act's broad definition of personal data includes not only traditional identifiers like names and email addresses but also more sensitive information such as browsing history, purchasing behaviors, and geolocation data. As with the GDPR, the CCPA mandates that businesses disclose their data practices clearly, allowing consumers to make informed decisions about their participation in digital advertising programs. The CCPA has raised the bar for data protection in the U.S., prompting businesses to reassess their data practices and provide consumers with greater control over their personal information (Sweeney, 2019).

While the GDPR and CCPA are among the most well-known data protection regulations, other jurisdictions around the world have also enacted or are in the process of developing privacy laws to address the challenges posed by digital advertising and tracking. Brazil's General Data Protection Law (LGPD), which came into effect in 2020, mirrors many aspects of the GDPR, particularly with regard to consent, transparency, and data subject rights. Similarly, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) requires businesses to obtain consent before collecting personal data and mandates that organizations be transparent about their data practices. In the Asia-Pacific region, countries such as Japan and South Korea have enacted their own privacy laws, which reflect a growing global trend toward strengthening data protection measures. Despite these efforts, inconsistencies in data protection laws across different regions create challenges for businesses that operate globally, requiring them to navigate a complex landscape of differing requirements and expectations (Greenleaf, 2019).

One of the major challenges businesses face in the digital advertising and tracking industry is ensuring compliance with a patchwork of global data protection regulations. Different jurisdictions have varying definitions of personal data, differing consent requirements, and divergent rules regarding data transfers across borders. For example, while the GDPR requires explicit consent for data collection, other regions like the U.S. rely more on opt-out mechanisms. This lack of uniformity creates compliance burdens for businesses that must adhere to multiple legal frameworks simultaneously. Furthermore, global data flows are often hindered by concerns over cross-border data transfers, especially in light of the GDPR's restrictions on transferring personal data outside the European Union unless certain conditions are met. To navigate these complexities, businesses must invest in legal expertise, adopt privacy-conscious technologies, and ensure that their data practices align with the most stringent regulations in the regions where they operate (Binns, 2018). As the regulatory environment continues to evolve, companies will need to remain agile and responsive to emerging privacy laws to avoid potential fines and reputational damage.

4. Privacy Concerns and Risks in Digital Advertising and Tracking

Digital advertising technologies have made it possible for companies to collect vast amounts of personal data, often without users' full awareness or explicit consent. This has led to concerns about surveillance, as the continuous tracking of users across multiple platforms enables advertisers to create detailed profiles based on individuals' online behaviors, preferences, and even personal circumstances. While this form of profiling allows for highly targeted advertising, it also raises significant privacy concerns. By compiling data from various sources, including browsing history, location data, and social media activity, advertisers can build profiles that reveal sensitive aspects of users' lives, such as their political beliefs, health conditions, and personal relationships. This creates a situation where users are constantly surveilled, with their every digital move being tracked and analyzed for the purposes of commercial gain. Critics argue that such extensive surveillance, often carried out invisibly in the background, undermines individuals' autonomy and can lead to manipulative practices, such as targeted political ads or exploitative marketing strategies that prey on users' vulnerabilities (Tufekci, 2018). Furthermore, the aggregation of this data across different platforms and devices raises concerns about the extent to which companies can control and use personal

information without the users' informed consent. In this context, the line between beneficial personalization and invasive surveillance becomes increasingly blurred.

Alongside privacy concerns, digital advertising and tracking also present significant data security risks. The collection, storage, and transfer of large volumes of personal data create numerous opportunities for breaches and unauthorized access. Advertisers, data brokers, and other third parties often retain vast amounts of consumer information, which can become prime targets for cybercriminals. Even with robust security protocols in place, the sheer volume and diversity of data increase the likelihood of vulnerabilities, making it difficult to safeguard all user information effectively. Data breaches in the advertising industry can have far-reaching consequences, as hackers could gain access to sensitive information such as financial data, health records, or behavioral patterns, which could be used for identity theft, fraud, or other malicious activities. Moreover, the interconnected nature of digital platforms makes it difficult to ensure the security of data as it is transferred between various entities, such as advertisers, data brokers, and analytics providers. In addition to the direct risks to individuals, such breaches undermine consumer trust in the advertising industry, which can have long-term economic repercussions for businesses (Kuner, 2020). As such, ensuring the integrity of user data has become a critical challenge, particularly as digital advertising increasingly relies on the use of personal and behavioral data.

One of the primary concerns around digital advertising is the lack of consumer control over personal data. In many cases, consumers are unaware of the extent to which their data is being collected or how it is being used in advertising. The use of tracking technologies often operates behind the scenes, without clear or easy-to-understand consent mechanisms. As a result, individuals may feel powerless in determining how their data is shared, who it is shared with, and for what purposes. Privacy policies, which are typically long and filled with legal jargon, do little to provide transparency, leaving users in the dark about the specific ways in which their data is being exploited. This lack of control can lead to frustration and distrust, especially when users are confronted with personalized ads based on deeply personal information. The ability to opt-out or manage data preferences is not always straightforward, and the process of withdrawing consent is often cumbersome or unclear. In some cases, users may feel coerced into accepting data collection practices in exchange for access to services or content, as opting out could mean losing access to certain features or benefits. These concerns highlight the need for more robust and transparent mechanisms that empower consumers to take control of their data and make informed choices about their participation in digital advertising (Sweeney, 2019).

5. Balancing Innovation and Privacy

Digital advertising plays a vital role in driving online commerce and fueling the modern economy. For many businesses, advertising revenue is a primary source of income, particularly for online platforms such as social media sites and search engines. The ability to target specific consumer segments allows advertisers to maximize the effectiveness of their campaigns and increase their return on investment. Personalization, made possible through data collection and behavioral tracking, enables businesses to deliver relevant ads to individuals who are most likely to engage with them. This not only benefits advertisers by increasing conversion rates but also enhances the user experience by providing content that aligns with personal interests. Moreover, digital advertising enables businesses to reach vast audiences at a fraction of the cost of traditional advertising methods, making it a crucial component of the global economy. The importance of advertising as a revenue stream has led many tech companies to prioritize data-driven advertising models, leading to significant investments in technology and infrastructure to collect, process, and analyze user data. As digital advertising continues to evolve, its economic impact will likely continue to grow, further embedding it into the fabric of online business models (Binns, 2018).

The ongoing tension between innovation in digital advertising and the need for privacy protection presents a complex challenge. On one hand, advertisers and technology companies argue that data-driven innovation leads to better services, more relevant content, and improved user experiences. Personalized advertising, in particular, allows for the delivery of highly targeted messages that are tailored to individual needs and interests, which can be beneficial for both consumers and businesses. On the other hand, there is growing concern that the rapid pace of technological innovation is outpacing the development of privacy protections, leaving individuals vulnerable to privacy violations and data misuse. New technologies such as artificial intelligence (AI) and machine learning have made it possible to collect and analyze more data than ever before, enabling advertisers to create even more refined and invasive advertising strategies. As a result, privacy advocates argue that the need

for stronger privacy regulations is more urgent than ever. This ongoing battle between innovation and privacy often leads to a delicate balancing act, where businesses must weigh the benefits of personalized advertising against the risks of violating users' privacy. The challenge lies in finding solutions that allow for the continued growth and innovation of digital advertising while safeguarding individuals' personal information and upholding their right to privacy (Regan, 2020).

In response to growing concerns about privacy, several privacy-enhancing technologies (PETs) have been developed to provide a middle ground between effective advertising and privacy protection. One such solution is contextual advertising, which focuses on delivering ads based on the content a user is currently engaging with, rather than relying on personal data or tracking past behaviors. This approach reduces the need for extensive data collection while still allowing advertisers to target relevant content to users based on their immediate interests. Another promising development is privacy-preserving analytics, which enables advertisers to gain insights from aggregated data without exposing individual-level information. Techniques such as differential privacy and federated learning allow for the analysis of large datasets while ensuring that personal information remains protected. Additionally, there are efforts to develop alternatives to third-party cookies, such as browser-based solutions that give users more control over how their data is shared with advertisers. These technologies offer a way to address privacy concerns without stifling the innovation and economic benefits that digital advertising provides. However, their widespread adoption will depend on the willingness of both advertisers and regulators to embrace new solutions and adapt to an evolving digital ecosystem (Greenleaf, 2019).

6. Future Directions and Policy Recommendations

As digital advertising continues to evolve, it is anticipated that data protection laws will also undergo significant developments to address emerging privacy challenges. Amendments to existing regulations, such as the General Data Protection Regulation (GDPR), are likely as policymakers work to adapt to new technologies and shifting consumer expectations. One area of focus for future amendments may include improving the enforcement mechanisms of data protection laws, as the complexity of global data flows presents challenges in holding companies accountable across jurisdictions. In addition, new privacy laws are expected to emerge, particularly in the United States, where the patchwork of state-level regulations like the California Consumer Privacy Act (CCPA) may eventually lead to federal privacy legislation. Such a law could harmonize data protection standards across the country and offer a more consistent framework for digital advertising practices. Globally, countries outside of the EU and U.S. are also expected to introduce or update privacy regulations, influenced by the GDPR and other existing frameworks. For instance, the Brazilian General Data Protection Law (LGPD) has already introduced GDPR-like provisions, and countries in Asia are considering or enacting similar laws to safeguard personal data. As these legal frameworks evolve, there will likely be increased focus on enhancing consumers' rights to control their data, ensuring that organizations provide greater transparency regarding data collection practices, and expanding the scope of regulatory bodies to address the growing challenges of data privacy in digital advertising (Greenleaf, 2019).

Technology is expected to play a pivotal role in reshaping the landscape of data privacy in digital advertising. Innovations such as artificial intelligence (AI) and blockchain offer promising solutions to improve privacy protections and change the dynamics of how data is collected and used in advertising. AI, for example, can be leveraged to develop more sophisticated privacy-preserving algorithms, such as differential privacy, which ensures that data is anonymized in a way that prevents the identification of individuals while still providing valuable insights for advertisers. Furthermore, AI-based systems could help advertisers deliver more contextually relevant ads without the need for invasive behavioral tracking, thereby reducing the reliance on personal data. Blockchain technology also presents significant potential for enhancing privacy in digital advertising by providing transparent and secure ways to handle consumer data. Blockchain's decentralized nature can allow users to maintain ownership of their data and control how it is shared, creating a more equitable data ecosystem. Consumers could potentially grant or revoke permission for data usage in a verifiable manner, providing a transparent record of consent and transactions that enhances trust between users and advertisers. Decentralized technologies such as federated learning, which allows data to remain on the user's device while still enabling machine learning algorithms to process it, could further reduce privacy risks. As these technologies evolve, they hold the potential to transform the digital advertising industry by fostering privacy-respecting approaches that still allow for effective personalization and targeted advertising (Regan, 2020).

For businesses, the key to navigating the evolving data privacy landscape will be to adopt a proactive approach to compliance, transparency, and user control. Companies should invest in robust data protection measures and ensure they are familiar with both current and upcoming regulations in the jurisdictions they operate in. This may include regular audits of data collection practices, updating consent mechanisms to be more transparent and user-friendly, and ensuring that all third-party vendors comply with relevant privacy standards. Adopting privacy-by-design principles in digital advertising campaigns, where privacy considerations are embedded into the development process, will also be crucial. Furthermore, businesses should embrace privacy-enhancing technologies such as contextual advertising or privacy-preserving analytics to reduce the reliance on personal data and minimize privacy risks. Regulators, on the other hand, must continue to evolve data protection laws to address emerging challenges in digital advertising, particularly the use of new technologies such as AI and blockchain. Future legislation should be flexible enough to accommodate rapid technological change while providing clear guidelines for businesses on how to comply with privacy requirements. Regulators should also consider strengthening cross-border cooperation and establishing frameworks for global data protection that ensure consistency across jurisdictions. Collaboration between businesses, policymakers, and privacy advocates will be essential to create a regulatory environment that fosters innovation while safeguarding individual privacy (Binns, 2018).

7. Conclusion

This article explored the complex relationship between data protection and digital advertising, highlighting the key privacy concerns and risks associated with technologies like behavioral tracking, cookies, and cross-device tracking. It discussed the essential principles of data privacy, including consent, data minimization, and user control, and examined the legal frameworks that govern data protection, such as the GDPR and CCPA. The article also identified challenges related to compliance with global privacy regulations, the risks posed by data breaches, and the growing concerns around surveillance and profiling. Despite these concerns, digital advertising remains a critical component of the modern economy, driving online commerce and enabling personalized experiences for consumers. The article further discussed the delicate balance between privacy and innovation, suggesting that future developments in privacy-enhancing technologies, such as AI and blockchain, could provide solutions to these challenges.

The evolving privacy landscape is already having a significant impact on the digital advertising industry. As data protection laws become more stringent, businesses in the advertising sector are increasingly required to adapt their practices to comply with privacy regulations. The emphasis on transparency, consumer control, and informed consent has forced companies to rethink how they collect and use data, with many adopting privacy-centric approaches to advertising. However, as businesses strive to maintain personalized advertising strategies, the challenge will be to find ways to innovate while respecting consumers' privacy rights. The GDPR, CCPA, and other regulations have made it clear that the protection of personal data is a priority, and as a result, digital advertising practices are likely to continue evolving in ways that prioritize consumer trust and privacy.

There are several key areas for future research in the field of data privacy and digital advertising law. One important area of focus is the impact of emerging technologies, such as AI, blockchain, and decentralized platforms, on privacy protection in advertising. Research could explore how these technologies can be implemented in ways that mitigate privacy risks while still supporting effective advertising strategies. Another area for further investigation is the global harmonization of privacy laws, with particular attention to how different regulatory regimes can be aligned to create a more consistent framework for digital advertising. Finally, there is a need for more empirical research on consumer attitudes toward data privacy in digital advertising, which could provide valuable insights into how consumers perceive their privacy rights and how they interact with privacy policies and consent mechanisms. As the digital advertising landscape continues to evolve, these areas of research will be essential in guiding the development of both regulatory frameworks and business practices that protect consumer privacy while fostering innovation (Sweeney, 2019).

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Binns, R. (2018). The Economics of Digital Advertising: A Guide for Marketers and Regulators. Oxford University Press.
Greenleaf, G. (2019). Global Privacy Law: A Comparative Analysis. Oxford University Press.
Kuner, C. (2020). Data Protection Law and International Jurisdiction: The Impact of the GDPR. Springer.
Regan, P. M. (2020). Privacy, Surveillance, and Digital Advertising: The Legal and Ethical Implications of Emerging Technologies. Routledge.
Sweeney, L. (2019). The Data Privacy Dilemma in Digital Advertising: A Consumer-Centric Perspective. MIT Press.
Tufekci, Z. (2018). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.