Consumer Privacy Concerns in Digital Marketing: A Review Paper

OLUWASANMI SEGUN ADANIGBO
Department of Business Management, University of the Cummberlands, USA

Abstract- ***Consumer privacy has emerged as a major concern in the rapidly evolving digital marketing landscape. This review paper examines the multifaceted issue of consumer privacy in the context of digital marketing, focusing on collection practices, consumer knowledge, and the ethical implications of data use so especially as businesses increasingly rely on sophisticated technology to collect and analyze customer data, questions of transparency, consent and the potential for abuse have become increasingly important the Paper says integrates current research and information gathering practices highlights the growing challenges and challenges to consumer privacy. It also explores different levels of consumer knowledge about data processing, and reveals important gaps in understanding that contribute to consumers' sense of vulnerability in addition to ethical considerations relating to the processing of personal data in consumer privacy in the context of targeted advertising to provide a detailed context of the current situation and to identify areas where further research and ethical guidance are needed to ensure consumer rights are protected.***

Indexed Terms- ***Digital Marketing, Consumer Privacy, Data Collection Practices, Consumer Awareness, Ethical, Implications, Transparency, Consent***

I. INTRODUCTION

In today's digital landscape, the collection and use of consumer data have become integral to the operations of businesses. This has led to significant concerns regarding consumer privacy, particularly in three key areas: data collection practices, consumer awareness, and the ethical implications of data use.

Data Collection Practices: The methods by which companies gather consumer data, including tracking cookies, online forms, and social media interactions, have raised questions about transparency and consumer consent. According to Tene and Polonetsky (2013), the extensive data collection practices employed by digital marketers often occur without the explicit knowledge or informed consent of consumers, leading to a potential breach of privacy.

Consumer Awareness: Consumer awareness about how their data is collected and used is another critical aspect. Research by Boerman, Kruikemeier, and Zuiderveen Borgesius (2017) shows that while consumers are increasingly aware of data collection practices, there remains a significant gap in understanding the full extent of data usage and the potential risks involved. This lack of awareness can lead to a false sense of security among consumers, making them more vulnerable to privacy breaches.

Ethical Implications of Data Use: The ethical considerations surrounding the use of consumer data in digital marketing are complex and multifaceted. As Nissenbaum (2011) argues, the use of personal data for targeted advertising raises ethical concerns about autonomy, manipulation, and the erosion of consumer trust. The ethical implications extend beyond legal compliance, touching on the moral responsibilities of marketers to protect consumer privacy and act transparently.

Digital marketing has become an indispensable tool in the contemporary business environment, enabling companies to reach and engage with consumers on a global scale. With the rise of the internet, social media, and mobile technologies, businesses have unprecedented access to vast amounts of consumer data. This data allows for highly targeted and personalized marketing strategies, which have proven to be significantly more effective than traditional approaches. As a result, digital marketing has transformed how companies communicate with their customers, driving innovation and competition across various industries.

Importance of Consumer Privacy

However, the growing reliance on consumer data in digital marketing has brought privacy concerns to the forefront. The collection, analysis, and use of personal information raise critical questions about consumer autonomy, consent, and the potential for misuse of data. As digital marketing practices become more sophisticated, the line between useful personalization and invasive surveillance becomes increasingly blurred. Consumer privacy has thus emerged as a critical issue, not only from a legal and regulatory perspective but also in terms of maintaining consumer trust and ensuring ethical business practices. Breaches of consumer privacy can lead to significant reputational damage for companies, legal penalties, and a loss of consumer confidence.

Purpose and Scope

The purpose of this review is to examine the multifaceted issue of consumer privacy within the context of digital marketing. Specifically, this paper will focus on three key areas: data collection practices, consumer awareness, and the ethical implications of data use. By synthesizing recent research and exploring current trends, this review aims to provide a comprehensive understanding of how these aspects interact and affect consumer privacy. The review will also highlight existing gaps in the literature and suggest areas for future research, contributing to the ongoing discourse on balancing innovation in digital marketing with the need to protect consumer privacy.

Aim and Objectives

The primary aim of this review is to critically analyze the current state of consumer privacy in digital marketing. The specific objectives are:

1. To explore the methods and practices used by companies to collect consumer data and the associated privacy concerns.
2. To assess the level of consumer awareness regarding data collection and its implications.
3. To examine the ethical challenges posed by the use of consumer data in personalized marketing strategies.
4. To identify gaps in the current research and propose directions for future studies.

Limitations

While this review provides a comprehensive overview of consumer privacy concerns in digital marketing, it is important to acknowledge certain limitations. The scope of this paper is confined to the examination of data collection practices, consumer awareness, and ethical implications. It does not delve into related areas such as data security or the technical specifics of data encryption. Additionally, this review is limited by the availability of recent academic literature, with a focus on studies published within the last decade. As the field of digital marketing evolves rapidly, some of the findings may be subject to change as new technologies and regulations emerge.

II. LITERATURE REVIEW

1. Data Collection Practices

Legal Aspects: GDPR and CCPA Compliance

The implementation of regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States has significantly impacted how businesses approach data collection. These laws require companies to obtain explicit consent from consumers before collecting personal data and to provide transparency about how that data is used (Voigt & von dem Bussche, 2017). However, the effectiveness of these regulations in truly protecting consumer privacy has been questioned. For instance, Jachim (2020) argues that while GDPR and CCPA have increased awareness of data privacy issues, enforcement remains inconsistent, and many companies still struggle with full compliance, particularly in adapting to the complex requirements for data management and reporting.

Technological Aspects: Cookies, Tracking Pixels, and Beyond

From a technological standpoint, the use of cookies, tracking pixels, and other data collection tools has become ubiquitous in digital marketing. These tools allow marketers to gather detailed information about user behavior, preferences, and demographics, often without the user's explicit knowledge (Roesner, Kohno, & Wetherall, 2012). Recent advancements in artificial intelligence and machine learning have further enhanced the ability to analyze and predict consumer behavior based on collected data. However,

the ethical implications of these practices are increasingly coming under scrutiny. According to Zwick and Knott (2020), the extensive use of tracking technologies raises serious concerns about the erosion of consumer autonomy and the potential for manipulative marketing practices.

2. Consumer Awareness

Consumer Behavior: Understanding and Misunderstanding Data Use

Despite the increasing use of sophisticated data collection techniques, consumer awareness of how their data is being used remains limited. Research by Martin and Murphy (2017) suggests that while consumers are generally aware that their data is being collected, they often do not fully understand the extent or the implications of this data collection. This gap in understanding can lead to what Acquisti, Brandimarte, and Loewenstein (2015) describe as the "privacy paradox," where consumers express concerns about privacy but do not take actions to protect themselves, often because they do not know how or because they perceive the benefits of data sharing to outweigh the risks.

Legal and Ethical Implications: The Role of Transparency

Transparency in data collection practices is critical for improving consumer awareness and trust. However, achieving true transparency is challenging, especially given the technical complexity of many data collection methods. Floridi (2018) points out that even when companies provide disclosures about their data practices, these disclosures are often too complex or vague for the average consumer to understand, thereby undermining the goal of informed consent. This highlights a significant gap in the current regulatory frameworks, which focus on the provision of information without ensuring that this information is accessible and meaningful to consumers.

3. Ethical Implications of Data Use

Ethical Considerations: Balancing Personalization and Privacy

The ethical implications of data use in digital marketing are profound, particularly in the context of personalized advertising. While personalization can enhance the consumer experience, it also raises questions about the boundaries of acceptable data use. According to Moor (2019), the use of personal data for targeting consumers based on their behavior, preferences, and vulnerabilities can be seen as a form of manipulation, particularly when consumers are unaware of how their data is being used. This creates a tension between the goals of marketers and the rights of consumers, suggesting the need for more robust ethical guidelines and industry standards.

Emerging Trends: The Shift Toward Ethical AI

As the use of AI in digital marketing grows, there is a pressing need to address the ethical challenges associated with AI-driven data collection and analysis. Mittelstadt, Allo, Taddeo, Wachter, and Floridi (2016) emphasize the importance of developing ethical AI frameworks that prioritize transparency, fairness, and accountability. However, there is still a significant gap in research on how these ethical principles can be practically implemented in marketing strategies, particularly in the context of balancing personalization with privacy.

Gaps in the Literature and Future Directions

While significant research has been conducted on data collection practices, consumer awareness, and the ethical implications of data use, several gaps remain.

- First, there is a need for more empirical studies that assess the effectiveness of current regulations like GDPR and CCPA in protecting consumer privacy, especially in diverse cultural and legal contexts.
- Second, more research is needed to explore how consumers perceive and respond to transparency initiatives, particularly in terms of their understanding and trust.
- Finally, the ethical challenges posed by emerging technologies such as AI require further exploration, particularly in developing actionable guidelines that can be integrated into industry practices.

III. THEORETICAL FRAMEWORK

- Privacy Paradox

The Privacy Paradox refers to the conflicting behavior where consumers express concern about their privacy but often fail to take actions to protect it. According to Acquisti, Brandimarte, and Loewenstein (2015), this paradox is a significant challenge in understanding

consumer behavior in the digital age. Consumers claim to value their privacy, yet they frequently share personal information online, either due to convenience or a lack of understanding of the potential risks. This paradox complicates efforts to design effective privacy protections, as consumer actions do not always align with their stated preferences.

- Trust Theory

Trust Theory is pivotal in understanding how consumers decide whether to share their personal information with companies. McKnight, Choudhury, and Kacmar (2002) suggest that trust in digital platforms is built on the perception of competence, benevolence, and integrity. When consumers trust that a company will handle their data responsibly, they are more likely to engage in online transactions and share personal information. However, any breach of this trust can lead to significant damage to the company's reputation and consumer loyalty, as highlighted by Beldad, de Jong, and Steehouder (2010).

- Regulatory Focus Theory

Regulatory Focus Theory (RFT), as proposed by Higgins (1997), explores how individuals approach decision-making processes based on two distinct motivational orientations: promotion and prevention. In the context of consumer privacy, RFT helps explain why some consumers are more vigilant about protecting their privacy (prevention-focused) while others may be more concerned with the benefits of sharing information (promotion-focused). This theory provides a useful lens for understanding the diversity of consumer responses to privacy policies and practices (Crowe & Higgins, 1997).

- Key Areas of Consumer Privacy Concerns
- Data Collection and Usage

Companies employ various methods to collect, store, and use consumer data, raising significant privacy concerns. According to Tene and Polonetsky (2013), the widespread use of tracking cookies, social media monitoring, and data analytics allows companies to gather extensive information about consumers' online activities. While these practices enable personalized marketing, they also pose risks related to data breaches and unauthorized access. The lack of transparency in data collection practices often leads to consumer distrust, as many users are unaware of how much data is being collected and for what purposes (Boerman, Kruikemeier, & Zuiderveen Borgesius, 2017).

- Consumer Awareness and Behavior

Consumer awareness of privacy issues is crucial in shaping online behavior. A study by Milne, Rohm, and Bahl (2004) found that while consumers are increasingly aware of privacy risks, their understanding of how to protect their personal information remains limited. This gap between awareness and action is a key component of the Privacy Paradox. Moreover, consumers often engage in privacy-compromising behaviors due to a lack of understanding of complex privacy policies or the perceived benefits of sharing information (Martin & Murphy, 2017).

- Legal and Ethical Considerations

The legal landscape surrounding consumer privacy is shaped by regulations such as the GDPR and CCPA, which aim to protect consumers by enforcing strict data protection standards. Voigt and von dem Bussche (2017) argue that these regulations have significantly increased corporate accountability and consumer rights. However, ethical considerations extend beyond legal compliance. Nissenbaum (2011) emphasizes that companies must also consider the broader moral implications of their data practices, such as the potential for discrimination, manipulation, and loss of consumer autonomy.

Legal Frameworks

The legal landscape for consumer privacy has evolved significantly with the introduction of comprehensive data protection regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

GDPR: Enforced since May 2018, the GDPR is a landmark regulation in the European Union that sets stringent standards for data protection and privacy. It grants consumers greater control over their personal data and imposes heavy penalties on companies that fail to comply (Voigt & von dem Bussche, 2017). The GDPR mandates that companies obtain explicit consent from individuals before collecting their data, ensure transparency about data usage, and allow consumers to access, correct, and delete their personal information. It has been praised for setting a high bar for data protection, fostering a culture of accountability, and enhancing consumer rights.

CCPA: Implemented in January 2020, the CCPA is a significant data protection law in California that provides similar protections as the GDPR but within a U.S. context. The CCPA allows consumers to know what personal data is being collected, to whom it is being sold, and provides them with the right to opt-out of the sale of their data (Voigt & von dem Bussche, 2017). While it represents a major step towards stronger privacy protections in the U.S., its scope and implementation are somewhat less comprehensive compared to the GDPR.

Both regulations reflect a growing recognition of the importance of consumer privacy and have significantly increased corporate accountability. They have also influenced data protection practices globally, prompting companies outside their jurisdictions to adopt similar standards to remain competitive and avoid legal risks.

Ethical Considerations

Beyond legal compliance, ethical considerations play a crucial role in shaping responsible data practices. According to Nissenbaum (2011), companies must address broader moral issues related to data privacy, such as:

Discrimination: The use of personal data can lead to discriminatory practices, especially when algorithms used for targeting or decision-making reflect biases present in the data or design. This can result in unfair treatment of individuals based on their race, gender, or socioeconomic status.

Manipulation: The ability to collect and analyze large amounts of data can be used to manipulate consumer behavior in ways that undermine autonomy. For example, targeted advertising may exploit vulnerabilities or psychological triggers to influence purchasing decisions, raising ethical concerns about consent and manipulation.

Loss of Consumer Autonomy: As companies gather and utilize extensive personal data, there is a risk of diminishing individual autonomy. Consumers may feel compelled to share their data due to the perceived benefits or because they lack a clear understanding of how their information will be used. This erosion of autonomy can be compounded by complex privacy policies that obscure how data is collected, shared, and used.

Nissenbaum (2011) argues that addressing these ethical concerns requires a commitment to transparency, fairness, and respect for individual rights. Companies should adopt ethical guidelines that go beyond legal requirements, ensuring that data practices align with broader moral values and respect consumer autonomy.

The legal and ethical considerations surrounding consumer privacy are critical to shaping responsible data practices in digital marketing. While regulations like the GDPR and CCPA have established important protections and increased corporate accountability, ethical considerations highlight the need for companies to consider the broader implications of their data practices. Addressing these concerns involves not only complying with legal standards but also fostering a culture of transparency and respect for consumer rights.

- Technological Solutions

Technology plays a dual role in consumer privacy, acting both as a protector and a potential threat. Encryption, anonymization, and blockchain technologies offer promising solutions for enhancing data security and protecting consumer privacy (Zyskind, Nathan, & Pentland, 2015). However, the rapid advancement of data analytics and AI also introduces new challenges, as these technologies can be used to re-identify anonymized data and exploit consumer vulnerabilities (Narayanan & Shmatikov, 2010). As Mittelstadt et al. (2016) highlight, there is a need for ongoing research and development of ethical AI frameworks to ensure that technological solutions are used responsibly in the digital marketing landscape.

Technology's role in consumer privacy is multifaceted, presenting both opportunities for enhanced protection and challenges that could compromise privacy. As digital marketing increasingly relies on advanced technologies, understanding these dual roles is crucial for safeguarding consumer information.

Encryption

Encryption is one of the most effective methods for protecting data from unauthorized access. By converting data into a code that can only be deciphered with a specific key, encryption ensures that even if data is intercepted, it remains unreadable to unauthorized parties. According to Zyskind, Nathan, and Pentland (2015), encryption techniques are vital for securing sensitive information during transmission and storage. For instance, Transport Layer Security (TLS) is widely used to encrypt data transmitted over the internet, ensuring secure communication between consumers and businesses. Despite its effectiveness, encryption is not foolproof. As encryption methods evolve, so do the techniques used by attackers to crack them, necessitating continuous advancements in encryption technology.

Anonymization

Anonymization involves removing or obscuring personal identifiers from data sets to prevent the identification of individuals. This technique is particularly useful in contexts where data is analyzed for patterns or trends without revealing individual identities. Narayanan and Shmatikov (2010) discuss the limitations of anonymization, highlighting that sophisticated data analytics can sometimes re-identify anonymized data by correlating it with other available information. Despite these challenges, anonymization remains a key strategy for protecting privacy, especially when combined with other privacy-preserving techniques.

Blockchain

Blockchain technology, originally developed for cryptocurrencies, has emerged as a promising solution for enhancing data security and privacy. By creating a decentralized and immutable ledger of transactions, blockchain ensures that data is tamper-proof and transparent (Zyskind, Nathan, & Pentland, 2015). In the context of digital marketing, blockchain can be used to verify the authenticity of data, track consent agreements, and manage permissions for data use. However, the scalability and integration of blockchain in existing systems pose significant challenges. As blockchain technology is still evolving, its full potential for protecting consumer privacy is yet to be realized.

Challenges with Advanced Technologies

While these technological solutions offer significant benefits, they also introduce new privacy challenges. The rise of data analytics and artificial intelligence (AI) has made it easier to process and analyze large volumes of data, but it also raises concerns about the re-identification of anonymized data and the exploitation of consumer vulnerabilities. For example, AI algorithms can analyze patterns and behaviors to make highly accurate predictions about individuals, potentially leading to privacy invasions (Narayanan & Shmatikov, 2010). Mittelstadt et al. (2016) emphasize the need for ethical AI frameworks to guide the development and application of AI technologies, ensuring that they are used responsibly and transparently.

Ethical AI Frameworks

As AI technologies become more integrated into digital marketing, there is a growing need for ethical guidelines to address privacy concerns. Mittelstadt et al. (2016) advocate for the development of ethical AI frameworks that prioritize transparency, fairness, and accountability. These frameworks should address issues such as data bias, informed consent, and the responsible use of AI in predicting and influencing consumer behavior. Ongoing research and dialogue are essential to create standards that balance the benefits of AI with the need to protect consumer privacy.

The technological solutions available for protecting consumer privacy—encryption, anonymization, and blockchain—offer valuable tools for enhancing data security. However, the rapid advancement of data analytics and AI presents new challenges that must be addressed through continuous innovation and ethical oversight. By developing robust privacy protection mechanisms and ethical guidelines, businesses can better safeguard consumer information and maintain trust in the digital marketing landscape.

IV. DISCUSSION

Emerging Trends

Artificial Intelligence (AI): AI is revolutionizing digital marketing by enabling more sophisticated data analysis, automation, and personalization. Machine learning algorithms can predict consumer behavior,

personalize marketing messages, and optimize campaigns in real-time. However, the extensive use of AI also raises significant privacy concerns. AI systems often require vast amounts of data to function effectively, which can lead to intrusive data collection practices. Moreover, AI algorithms can inadvertently reinforce biases present in the data, potentially leading to discriminatory outcomes (Binns, 2018). As AI technology continues to evolve, ensuring that its use aligns with privacy principles and ethical standards is crucial.

Big Data Analytics: The proliferation of big data has transformed how businesses understand and engage with their customers. By analyzing large datasets, companies can uncover insights about consumer preferences, behaviors, and trends. While this can enhance the relevance of marketing efforts and improve customer experiences, it also poses risks related to data security and privacy. The aggregation and analysis of vast amounts of personal information can make individuals more vulnerable to data breaches and misuse. Companies must implement robust data protection measures and be transparent about how data is used to mitigate these risks (Kitchin, 2014).

Personalized Marketing: Personalization has become a key strategy in digital marketing, allowing companies to deliver tailored content and offers to individual consumers. This approach can enhance customer engagement and satisfaction by providing relevant experiences. However, the depth of personalization often relies on extensive data collection, which can encroach on privacy. Balancing the benefits of personalization with the need for privacy protection is a significant challenge. Consumers may feel uneasy about how much data is collected and how it is used to tailor their experiences, raising concerns about data transparency and consent (Lambrecht & Tucker, 2019).

Challenges and Opportunities

Challenges in Balancing Personalization and Privacy: One of the primary challenges marketers face is striking a balance between delivering personalized experiences and respecting consumer privacy. Personalization requires access to detailed consumer data, which can be perceived as invasive. Marketers must navigate this tension by ensuring that data collection practices are transparent and that consumers have control over their information. Privacy concerns can also arise from the potential for data breaches and misuse, making it essential for companies to implement robust security measures and communicate their data practices clearly (Tufekci, 2014).

Opportunities for Enhancing Consumer Trust: Despite the challenges, there are significant opportunities for enhancing consumer trust through responsible data practices. Companies that prioritize transparency, provide clear information about data usage, and offer robust data protection measures can build stronger relationships with their customers. Implementing privacy by design principles, where privacy considerations are integrated into the development of new technologies and processes, can also enhance trust. Additionally, engaging with consumers to obtain informed consent and allowing them to manage their data preferences can demonstrate a commitment to respecting their privacy (Solove, 2021).

Innovative Privacy Solutions: Emerging technologies offer innovative solutions for protecting consumer privacy while enabling effective marketing. For example, privacy-preserving techniques such as differential privacy and federated learning allow companies to analyze data without compromising individual privacy (Dwork & Roth, 2014; McMahan et al., 2017). These approaches can help reconcile the need for data-driven insights with the imperative to safeguard consumer information. As these technologies develop, they present opportunities for marketers to adopt privacy-conscious practices that align with evolving consumer expectations and regulatory standards.

The rapid advancements in AI, big data analytics, and personalized marketing present both opportunities and challenges for digital marketers. While these technologies offer powerful tools for enhancing consumer engagement and optimizing marketing efforts, they also raise significant privacy concerns. Balancing the benefits of personalization with the need for privacy protection requires thoughtful strategies and a commitment to transparency. By embracing innovative privacy solutions and prioritizing consumer trust, marketers can navigate these challenges and

build stronger, more ethical relationships with their customers.

CONCLUSION

Summary

This review has explored the complex landscape of consumer privacy concerns in digital marketing, focusing on the technological solutions and legal and ethical considerations that shape current practices. We examined how encryption, anonymization, and blockchain technologies contribute to safeguarding consumer privacy while acknowledging the new challenges introduced by advancements in AI and big data analytics. Legal frameworks such as the GDPR and CCPA play a crucial role in enhancing consumer protection, but ethical considerations extend beyond compliance to address issues of discrimination, manipulation, and consumer autonomy. Emerging trends like AI, big data, and personalized marketing offer both opportunities and challenges in balancing personalization with privacy concerns.

Future Directions

Future research should address several key areas to advance our understanding of consumer privacy in digital marketing:

1. Evolving Privacy Technologies: Research into emerging privacy-preserving technologies, such as differential privacy and federated learning, is essential. Studies should explore how these technologies can be integrated into marketing practices without compromising effectiveness (Dwork & Roth, 2014; McMahan et al., 2017).
2. Ethical AI Frameworks: Further investigation into ethical frameworks for AI is needed to ensure responsible use in marketing. This includes developing standards for transparency, fairness, and accountability in AI-driven marketing practices (Mittelstadt et al., 2016).
3. Consumer Perceptions and Behavior: Understanding how consumers perceive and react to privacy practices and personalized marketing is crucial. Research should focus on consumer attitudes towards data collection and privacy policies, and how these attitudes influence behavior (Lambrecht & Tucker, 2019).
4. Regulatory Impact: Examining the long-term effects of regulations like the GDPR and CCPA on both businesses and consumers can provide insights into their effectiveness and areas for improvement. Comparative studies across different regions can also highlight best practices and challenges in data protection (Voigt & von dem Bussche, 2017).

Implications for Practice

Marketers: To navigate the complexities of consumer privacy, marketers should adopt a transparent approach to data collection and use. Implementing privacy by design principles and ensuring that consumers are informed and have control over their data are crucial for building trust and maintaining ethical standards. Personalization strategies should be balanced with privacy considerations to avoid overstepping boundaries and causing consumer discomfort.

Policy-Makers: Policy-makers need to continue evolving data protection regulations to address emerging technologies and privacy challenges. They should also focus on harmonizing regulations across jurisdictions to simplify compliance for global businesses and enhance protection for consumers.

Consumers: Consumers should stay informed about their privacy rights and the data practices of the companies they engage with. Advocating for transparency and control over personal data can help drive positive changes in digital marketing practices and ensure that their privacy preferences are respected.

Conclusion

In summary, while technological advancements in digital marketing offer significant benefits, they also pose substantial privacy challenges. Addressing these concerns requires a multi-faceted approach involving robust technological solutions, comprehensive legal frameworks, and ethical practices. By focusing on these areas, stakeholders can work together to enhance consumer privacy, build trust, and foster a responsible digital marketing environment.

REFERENCES

[1] Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of

information. *Science*, *347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

[2] Beldad, A., de Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Computers in Human Behavior, 26(5), 857-869. https://doi.org/10.1016/j.chb.2010.03.013

[3] Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. Journal of Advertising, 46(3), 363-376. https://doi.org/10.1080/00913367.2017.1339368

[4] Crowe, E., & Higgins, E. T. (1997). Regulatory focus and strategic inclinations: Promotion and prevention in decision-making. Organizational Behavior and Human Decision Processes, 69(2), 117-132. https://doi.org/10.1006/obhd.1996.2675

[5] Floridi, L. (2018). Soft ethics and the governance of the digital. *Philosophy & Technology*, *31*(1), 1-8. https://doi.org/10.1007/s13347-018-0303-9

[6] Higgins, E. T. (1997). Beyond pleasure and pain. American Psychologist, 52(12), 1280-1300. https://doi.org/10.1037/0003-066X.52.12.1280

[7] Jachim, M. (2020). The effectiveness of GDPR and CCPA in the global context. *Journal of Data Protection & Privacy*, *3*(2), 130-145. https://doi.org/10.2139/ssrn.3452399

[8] Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135-155. https://doi.org/10.1007/s11747-016-0495-4

[9] McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334-359. https://doi.org/10.1287/isre.13.3.334.81

[10] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), 1-21. https://doi.org/10.1177/2053951716679679

[11] Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. Journal of Consumer Affairs, 38(2), 217-232. https://doi.org/10.1111/j.1745-6606.2004.tb00865.x

[12] Moor, J. H. (2019). The ethics of privacy in the age of big data. *Ethics and Information Technology*, *21*(2), 73-83. https://doi.org/10.1007/s10676-019-09504-1

[13] Narayanan, A., & Shmatikov, V. (2010). Myths and fallacies of "personally identifiable information." Communications of the ACM, 53(6), 24-26. https://doi.org/10.1145/1743546.1743558

[14] Nissenbaum, H. (2011). A contextual approach to privacy online. Daedalus, 140(4), 32-48. https://doi.org/10.1162/DAED_a_00113

[15] Roesner, F., Kohno, T., & Wetherall, D. (2012). Detecting and defending against third-party tracking on the web. In *Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI'12)* (pp. 155-168). USENIX Association.

[16] Tene, O., & Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property, 11(5), 239-273. https://doi.org/10.2139/ssrn.2149364

[17] Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. *Springer International Publishing*. https://doi.org/10.1007/978-3-319-57959-7

[18] Zwick, D., & Knott, J. (2020). Surveillance capitalism and the market for data: A political economy of personal information. *Journal of Business Ethics*, *167*(2), 233-243. https://doi.org/10.1007/s10551-019-04332-y