

From “Unbounded Tracking” to “Bounded Trust”, Data Privacy Protection Reshapes Personalized Marketing Approaches

Yingxuan Zhang *

School of Public Administration, Dongbei University of Finance and Economics, Dalian, China

* Corresponding Author Email: shuih122@outlook.com

Abstract. As information private security is gaining more weight and excellent laws and regulations are being put into effect, the panorama of individual marketing is changing drastically. A detailed analysis of the impact of data privacy security on personal advertising not only provides companies with useful data for developing marketing strategies but also aids administrations in refining regulation policies, which makes this analysis really good for valuable advice. This paper examines its numerous effects on suited advertising applying case studies and books research. And when it turns out that knowledge private security is more of a motivating measure than a typical restraint, it is intended to lead organizations on to devote more time and resources to establishing and improving several laws and regulations in order to create a pleasant, peaceful, and socially respected market environment. In this paper, suggestions and references are provided for the rational use of relevant air pressure data for personalized marketing.

Keywords: Data privacy protection, personalized marketing, bounded trust.

1. Introduction

The vigorous development of the digital economy has made data the “new oil”, businesses are increasingly using data eco-systems to collect, distribute, process, and consume data in response to the growing need to use data for economic gain so that personalized marketing has become a core engine for corporate growth [1]. However, frequent incidents of excessive data collection, misuse, and breaches have triggered global privacy concerns.

In order to protect the basic rights of citizens, prevent privacy from being violated, and regulate the development of the digital economy, many countries and regions around the world have introduced relevant regulations, such as the General Data Protection Regulation (GDPR) of the European Union in 2018, the California Consumer Privacy Act (CCPA) of California, the United States, and the Personal Information Protection Law (PIPL) of China. Their introduction marks the entry of global digital governance into a “new stage”. Although the focus of these laws is different, they share the fundamental common concept and principle that the virtual space is not a “lawless place”, and any violation of privacy should be punished.

Take GDPR as an example, data from “GDPR Enforcement Tracker” shows that in the early stage, there were relatively few enforcement cases [2]. However, as time went on, enforcement activities became increasingly frequent, with several “sky-high fines” amounting to hundreds of millions of euros, indicating that regulatory authorities have entered a mature stage of enforcement. From an industry perspective, technology and internet companies are the “hotspots” of fines, frequently being hit with huge fines due to data security breaches and cross-border data transmission issues. Besides, the telecommunications and financial services industries are also frequently fined. In summary, industries with larger data volumes, more sensitive data types, and deeper reliance on data in their business models face higher compliance risks and potential fines.

This article aims to study how enterprises should balance marketing effectiveness and compliance requirements in the seemingly contradictory context of “whoever gets the data gets the world” and “whoever protects privacy gets trust”, and to explore whether privacy protection will really hinder the development of personalized marketing.

2. The Connotations of Data Privacy Protection and Personalized Marketing

2.1. Evolution of Personalized Marketing

The development of personalized marketing has always been closely linked to technological innovation and changes in consumer demand, and its evolution can be clearly divided into three key stages. During the mass marketing stage, enterprises mainly relied on traditional media such as newspapers, television, and radio to carry out marketing activities by “casting a wide net”. The same marketing information was transmitted to all potential audiences, and users could not be distinguished, resulting in low efficiency and serious waste of resources.

After the rise of database technology, personalized marketing entered a new stage. Enterprises began to collect basic information of consumers and store it in the database, and classify consumers through simple analysis, and then carry out targeted marketing.

After entering the 21st century, the rapid development of technologies such as big data and artificial intelligence has promoted personalized marketing to enter the stage of big data-driven precision advertising [3]. Companies are able to collect massive amounts of consumer data, covering consumers' browsing behavior, social interaction, geographic location and other multi-dimensional data. Through advanced algorithms and models to conduct in-depth analysis of these data, enterprises can build accurate user profiles and achieve accurate advertising. Certain marketing has already significantly increased sales productivity and customer data as a result of the increased focus on data collection and consumer monitoring.

2.2. The Rise of Data Privacy Protection

There has been a rapid rise in global reputation of data security defense in recent years, mostly as a result of repeated incidents involving data protection. As the digitalization process accelerates, personal data circulates extensively across various platforms and institutions, making data security risks increasingly prominent. Some internet enterprises, due to inadequate security protection measures, have suffered leaks of sensitive user information such as phone numbers, ID card numbers, and consumption records. This leaked data is often exploited by criminals for illegal activities, including sending promotional spam messages, making harassing calls, and even committing telecom fraud. While suffering from property losses and psychological distress, consumers have also shown a growing concern for and demand for data privacy protection, and they have successively called for strengthened protection of personal data.

3. The Impacts of Data Privacy Protection on Personalized Marketing

3.1. Restructuring of the Data Foundation

3.1.1. Reduction in data collection scope and precisiong

Under the stringent constraints of data privacy protection regulations, the reinforcement of the “notice-and-consent” rule mandates that enterprises must inform users in a clear, explicit and comprehensible manner regarding the purpose, scope, methods, and usage of data collection. Furthermore, user consent must be active, explicit, and specific; it cannot be obtained through pre-ticked boxes, implied terms, or similar mechanisms. Any deployment of web-tracking technology that fails to meet these standards for valid user consent is considered a violation [4]. This paradigm shifts grants users' greater autonomy over data authorization but simultaneously increases the difficulty for enterprises to obtain data. However, businesses are only permitted to collect and use data when it is definitely important for a particular promotion function in accordance with the data decrease process, which forbids the gathering of foolish information. By minimizing both the size and the depth of the data used to create complete user profiles, this need fundamentally alters how information is collected and used in marketing works.

3.1.2. Increase in data costs and compliance risks

Compliance challenges and business data acquisition prices have both soared at the same time. These changes drastically affect the performance and development of the business. Businesses may spend significant resources in improving data safety measures, creating user-pleasant authorization interfaces, and streamlining data collection procedures to accomplish their lawful obligations and get a good user data. Then, they must enhance user willingness to share knowledge by providing better goods and services and exciting prizes. These activities both increase the cost of architecture and human resources. Data storage also costs a lot, and it also requires a large amount of money to protect consumer information from unauthorized access by subsequent events [5].

Significant limitations have created strict standards for data running businesses in terms of conformity dangers. If they violate the rules, they may encounter significant legal and financial sanctions, which could hurt brand reputation, tarnish consumer trust, and even have an impact on market competitiveness and lengthy-term growth. Furthermore, as rules modify and police regulations become greater, conformity requirements continue to rise. Due to this ongoing change, the compliance risk is getting more and more difficult, which calls for regular study prices to record legal changes and adjust data methods quickly to ensure organizations be compliant with the most current requirements. When AI algorithms operate as black boxes, it becomes challenging for advertisers, consumers, and even regulators to understand and scrutinize the underlying mechanisms driving advertising decisions [6]. This creates significant difficulties for enterprises in meeting regulatory demands for transparency in data processing, thereby amplifying compliance risks.

3.2. Dilemmas in Marketing Effectiveness

Protection of data privacy also has certain detrimental effects on real marketing results. This essay analyzed two examples in order to obtain additional understanding. The first is that in its 2021 iOS update, Apple introduced the App Tracking Transparency(ATT) framework, which mandates that apps get express user consent before tracking user data. Many consumers chose to reject app tracking when this framework was put into place. In terms of the type of corporate data strategy, Apple belongs to the type that imposes strict restrictions on the use and monetization of shared data. The launch of the “ATT” framework is a typical manifestation of proactive privacy innovation. This move directly broke the data foundation of Meta and other companies that rely on “unbounded tracking” to carry out personalized marketing models [7]. Platforms like Meta were greatly damaged by this, and the development of advertising income was noticeably slowed. Reduced ad reach and decreased marketing efficacy were among the problems experienced by companies who rely on Meta’s advertising platform.

In addition to Apple, Google has also officially announced that its Chrome browser will gradually phase out support for third-party cookies starting in January 2025. For companies that rely on third-party cookies for data collection and user tracking, this means that traditional data collection methods will no longer be available, the scope of data collection will be greatly reduced, especially the acquisition of user behavior data across platforms and websites will become extremely difficult, and the accuracy of data will be seriously affected. If enterprises fail to adjust their data collection strategies in time, they will face problems such as a shortage of data resources and a blurred user profile, which will affect the accuracy and effectiveness of personalized marketing.

3.3. The “Double-Edged Sword” Effect

The impact of data privacy protection on personalized marketing is not entirely negative but rather exhibits a “double-edged sword” effect. Businesses cannot conduct marketing activities by transmitting information without authorization, and marketing content must focus on areas that genuinely meet user needs, reducing the distraction of irrelevant advertisements. Respecting customers and keeping their private both contribute to greater price. Once they are informed that a business is effectively preserving their data and only using it within authorized restrictions to offer personalized services, users become more willing to work with them. They probably also frequently

offer more related data in order to get better personal knowledge. This trust-based communication supports longer-term private brand work, creating a noble cycle that promotes lengthy-term private brand creation as well as boosting customer loyalty and satisfaction. Although private security reduces marketing success in the short term, it does improve the users' experience, strengthen business confidence, and establish the basis for a extended-term development of personal marketing in the long run.

4. The Path Forward: Transformation Strategies for Personalized Marketing in the New Privacy Norm

Personal safety promotes the development of personalisation as a more developed form as opposed to the final product. In a world where data privacy protection is a popular topic, firms may break free of the restrictions of archaic types to make lasting personal brand in the new standard. Change is necessary across all three dimensions: beliefs, approaches, and systems in order to create a fresh specific marketing strategy that is based on trust, grounded in obedience, and driven by value exchange.

4.1. Paradigm Shift for Enterprises

4.1.1. From “data appropriation” to “value co-creation”

The core logic of the traditional personalized marketing model is “data appropriation”, where enterprises collect user data through various means as extensively as possible to achieve precise marketing, often neglecting user privacy needs and data sovereignty. In the new privacy norm, enterprises must view users as equal partners, exchanging value for user trust and willingness to share data. Incentives such as membership programs, premium content, and discounts can guide users to voluntarily register and provide data, offering clear value in return and constructing a marketing ecosystem based on mutual benefit. The user trade-off between “privacy and convenience” is essentially driven by “value perception”—users are only willing to compromise when privacy concessions are exchanged for high practical value. If the platform fails to provide differentiated, high-quality services, user willingness to concede privacy decreases significantly [8]. Enterprises must make users feel that sharing data yields tangible benefits or better service experiences, thereby enhancing their willingness to share data. This represents a fundamental shift from attempting to “own” data towards “earning” user trust and data-sharing willingness through value provision.

4.1.2. Technology enablement: application of privacy-enhancing technologies (PETs)

PETs refer to a category of technologies that enable data value extraction and utilization while protecting personal data privacy. Their core advantage lies in providing support for personalized marketing without directly accessing or exposing raw user data. In data processing, “Selective Differential Privacy (DP)” technology can be introduced. Its core principle involves adding a calibrated amount of “noise” to aggregated, truly sensitive datasets, making it impossible for attackers to reverse-engineer and identify specific individual user information through analysis of the aggregated data, while ensuring the overall trends and statistical characteristics of the aggregated data remain largely unaffected. This “selective” application significantly reduces computational overhead. This technique can protect user privacy while providing enterprises with effective data insights to support personalized marketing decisions. Likewise, selective DP applies noise only to truly sensitive training steps, reducing overhead and preserving more utility [9].

4.1.3. Method innovation: personalization beyond behavioral tracking

In commercial practice, the synergy between privacy compliance and marketing effect can also be achieved through marketing innovation, relying on contextual marketing. Contextual marketing does not require tracking users' cross-platform, long-term behavior, but focuses on users' current scenarios (such as content, time, and immediate needs), and binds advertisements to scenario needs to achieve accurate push. As the practice of ProMark framework in near-field marketing shows, it relies on short-

range communication technologies such as Bluetooth and NFC to enable witness devices (such as beacons) to be accurately deployed according to the type of marketing scenario - placed at the entrance in the store diversion scenario, and close to the target commodity in the product diversion scenario. Only when consumers enter the corresponding physical scenario, the marketing interaction is triggered, and the information strongly associated with the real-time scenario is pushed, completely getting rid of the dependence on the tracking data such as users' past browsing records and cross-platform behaviors [10].

4.2. Policy Formulation: Safeguarding the Compliant Development of Personalized Marketing

Amid growing data privacy protections, the healthy transformation of personalized marketing relies not only on internal corporate strategy and innovation but also on a supportive policy framework that offers clear guidance and assurance. Well-targeted policies can standardize corporate data practices, mitigate privacy risks, unleash the value of data as a productive factor, and create space for compliant innovation—ultimately fostering a virtuous cycle where enterprise experimentation, policy guidance, and industry standards reinforce one another.

4.2.1. Refining laws, regulations and standard systems

Although a core global privacy framework has emerged—exemplified by the GDPR, CCPA, and PIPL, but they remain overly broad and lack on details. Because they are conscious of their actual limits, businesses struggle with true compliance as a result of this question. So, stricter regulations must be in place as soon as possible to make sure that elected representatives and heirs are aware of what is and is not permitted. The company in which people write context-delicate tips for new models is based on now established regulations. Creating common compliance requirements for advertising targeting, individuals monitoring, and efficiency research should also be encouraged by business organizations and leading companies. These work may help Small and Medium-sized Enterprises (SMEs) understand the complexity of the rules and avoid breaches, which are often lacking in conformity skills. A properly-defined set of regulations and standards charm fosters a stable, reliable policy atmosphere, strengthens the police, and stops “data misuse” under the pretext of “personalized marketing”.

4.2.2. Encouraging technological development and infrastructure development

User data platforms and protection- increasing technologies are important players in the privateness- conscious marketing change. Due to limited R&D resources and large upfront costs, several small and medium- small businesses are unable to simply participate in cutting- edge solutions like variable protection, united understanding, or advanced first- party data management systems.

Political opportunities and resources can play a major part in closing this gap, and public policy may support. Companies that are building or developing new privateness- systems may be able to create a “Special Bank for Privacy Protection and Personalized Marketing Development” accounts. Also, the state does encourage the development of “public information infrastructure”, such as available-access websites for companies, to significantly lower SMEs’ costs for information acquisition and management. Policy support and financial assistance can contribute to the development of privacy-associated technologies, aiding in the development of specific marketing. Also, it lowers the passage challenge for SMEs, supporting a field- wide change from “extensive advertising” to “obedient and specific marketing”, encouraging the continued growth of private marketing. In spite of the dialogue that followed, it is obvious that data security protection laws will not only prevent the finished, non- obedient, and unsustainable conventional designs but even stop the development of customized advertising. It calls for businesses to improve their techniques and apply effective change, and raises the bar for selling to a new level based on trust, accountability, and benefit package. the website development industry.

5. Conclusion

From the above discussion, it is clear that data privacy protection regulations will not curb the better development of personalized marketing, but will eliminate the closed, non-compliant and unsustainable traditional models. It forces enterprises to carry out technological upgrading and strategic transformation and promotes marketing to a new stage based on trust, transparency and value exchange.

Businesses must now prioritize investing in and modernizing data privacy protection technology. Additionally, they might set up a specialized company to manage this work, guaranteeing that the staff and procedures are uniform and expert. Also, they can create their own platforms to gather, store, and use this data to give customers better service.

Future research can expand the research scope appropriately, strengthen case studies in industries with strict regulations such as healthcare and finance, analyze the impact of different industry data characteristics on the collaborative model of personalized marketing and privacy protection, and construct industry-specific solutions.

From the perspective of consumers, by combining psychological and sociological theories, it is possible to study the differences in responses of consumers with different demographic characteristics (such as age, educational level), digital literacy, and privacy concern to privacy protection policies and personalized marketing. Establish a correlation model of “consumer segmentation - privacy strategy matching - marketing effect optimization” to enhance the relevance and practicality of the research conclusions.

References

- [1] Burmeister Fabian, Kurtz Christian, Schirmer Ingrid. Governing information privacy in data ecosystems with architectural thinking. *Electronic Markets*, 2025, 35 (1): 67 - 67.
- [2] GDPR Enforcement Tracker. Statistics and insights on GDPR fines. CMS.Law, <https://www.enforcementtracker.com/>. 2024.
- [3] Chandra S, Verma S, Lim W M, Kumar S, Donthu N. Personalization in personalized marketing: Trends and ways forward. *Psychology & Marketing*, 2022, 39 (8): 1529 - 1562.
- [4] Martínez David, Molero Aniol, Calle Eusebi, Ametller Dolors Canals, Jové Albert. Large-scale web tracking and cookie compliance: Evaluating one million websites under GDPR with AI categorization. *Journal of Network and Computer Applications*, 2025, 242: 104222 - 104222.
- [5] Goldfarb A, Que V F. The economics of digital privacy. *Annual Review of Economics*, 2023, 15 (1): 267 - 286.
- [6] Alhitmi H K, Mardiah A, Al-Sulaiti K I, Abbas J. Data security and privacy concerns of AI-driven marketing in the context of economics and business field: an exploration into possible solutions. *Cogent Business & Management*, 2024, 11 (1): 2393743.
- [7] Quach S, Thaichon P, Martin K D, Weaven S, Palmatier R W. Digital technologies: tensions in privacy and data. *Journal of the academy of marketing science*, 2022, 50 (6): 1299 - 1323.
- [8] Zhang J H, Koivumäki T, Chalmers D. Privacy vs convenience: Understanding intention-behavior divergence post-GDPR. *Computers in Human Behavior*, 2024, 160: 108382.
- [9] Feretzakis G, Vagena E, Kalodanis K, Peristera P, Kalles D, Anastasiou A. GDPR and Large Language Models: Technical and Legal Obstacles. *Future Internet*, 2025, 17 (4): 151.
- [10] Hoang Anh-Tu, Carminati Barbara, Ferrari Elena. ProMark: Ensuring Transparency and Privacy-Awareness in Proximity Marketing Advertising Campaigns. *IEEE Transactions on Dependable and Secure Computing*, 2025, 22 (3): 2119 - 2131.