Asian Journal of Research in Education and Social Sciences
e-ISSN: 2682-8502 | Vol. 7, No. 3, 511-521, 2025
https://asianscholarsnetwork.com/asnet-journals

Exploring How Targeted Advertising Influences Individual Behavior Through the Facebook Leak Incident

Wang Peng[1], Norhayati Hussin[1*], Masitah Ahmad[1]

[1] School of Information Science, College of Computing, Informatics and Media, Universiti Teknologi MARA Cawangan Selangor, Kampus Puncak Perdana, Shah Alam, Selangor, Malaysia

*Corresponding Author: yatihussin@uitm.edu.my

Received: 21 February 2025 | Accepted: 9 April 2025 | Published: 30 April 2025

DOI: https://doi.org/10.55057/ajress.2025.7.3.44

Abstract: *This article analyzes the Facebook data breach incident to explore how businesses utilize user data for precise marketing in the era of big data. It begins by explaining the concept and technical framework of targeted advertising, covering key steps such as data collection, user profiling, personalized content creation, and algorithmic matching for ad delivery. The paper then provides a detailed analysis of the entire Facebook incident, including how Cambridge Analytica illegally accessed user data, used big data technologies like the five-factor model for personality analysis to create user profiles, and designed customized content for different user groups to influence their voting behavior. This incident exposed vulnerabilities in Facebook's data protection and raised global concerns about personal data security and privacy protection, leading to increased regulatory oversight of tech companies and forcing Facebook to reform its policies and strengthen data management. The article concludes by discussing the advantages and risks of targeted advertising, emphasizing the need to balance protecting privacy and leveraging the benefits of big data. It suggests that creating a safe, transparent environment for big data applications requires strengthening regulations, raising public awareness, and encouraging corporate self-regulation.*

Keywords: Big Data, Data Breach, Facebook, User Personality Analysis, Influencing User Behavior

1. Introduction

Sivarajah et al. (2020, pp. 163-179) recommended personal data has become an indispensable part of today's society, permeating almost every aspect of our daily lives. From the moment we unlock our phones in the morning to the health monitoring before we sleep at night, various types of data surround our lives. At work, we generate various data, including project progress reports, emails, and online meeting records. We share data about our personal preferences, interests, and interactions on social networks. Daily shopping activities also generate much data, including purchase history, preferences, and payment methods. Xiao (2019, pp. 45-52) confirms the hypothesis that data about our health, location, and entertainment preferences are also inadvertently recorded.

Personal data is not merely a collection of numerical records; it reflects our behavioral patterns, preference trends, and lifestyle habits. Thus, the management and utilization of personal data become extremely important. It helps us understand ourselves more deeply and provides valuable support for personalized services, health management, and marketing. In a recent study of reaction times (Zongyu Song, 2022, pp.158) the privacy and security of personal data cannot be overlooked. It is essential to ensure that data is not misused or leaked to protect personal information security and rights. The management and protection of personal data have become a global issue. Frequent data breaches have prompted increased attention to data security and privacy rights. Voigt and Von dem Bussche (2017) discuss that governments and regulatory bodies are enacting stricter data protection regulations, and the public is encouraged to enhance their awareness of data protection, learn to handle personal data securely and exercise their rights to control information. Many countries and regions, such as the European Union, have implemented strict data protection laws, such as the General Data Protection Regulation (GDPR).

In the era of big data, our behavioral habits are being quietly analyzed and interpreted, further influencing our decisions and lifestyles. We should treat behavioral data cautiously and remain vigilant to avoid undue influence and manipulation. At the same time, we should learn to utilize the conveniences brought by big data while protecting privacy to enjoy an efficient life. Moreover, big data analysis on social networks and entertainment platforms quietly changes our behavior. In 2021, Tariq compared reaction times, analyzing interaction records, preferences, and social networks to provide more attractive and personalized content, increasing our engagement. This personalized content delivery and social interaction may affect our views and attitudes and even shape our values and behaviors. The Facebook data breach incident serves as a reminder to pay attention to personal data security. In 2018, the Cambridge Analytica scandal broke out, revealing vulnerabilities in Facebook's data protection and sparking global concern over data privacy and social media responsibility.

This article delves into the Facebook data breach incident, exploring how targeted delivery utilizes user data to influence user behavior. In a recent study of reaction times (Chandra, 2022) initially, data acquisition serves as the starting point, encompassing information provided by users (such as personal profiles and interests) and data generated while using Facebook (such as likes, comments, and browsing history). These data lay the foundation for data analysis and the construction of user profiles. Subsequently, through complex algorithms, Facebook analyzes these data to identify users' behavioral patterns, preferences, and potential needs, thereby constructing detailed user profiles. With these profiles, Facebook can devise targeted delivery schemes, generating personalized content (such as advertisements, news, and posts) to capture user attention and increase engagement. Zuboff (2019) found that ultimately, the content of these targeted deliveries influences users' decisions and behaviors, such as prompting purchases or changing views on certain issues.

Through the above analysis, we not only recognize the powerful function of targeted delivery but also become aware of the potential data security issues it may trigger. The Facebook data breach incident exposed flaws in personal information protection, sparking public concern over privacy security. Meanwhile, the impact of targeted delivery on people's lives and behaviors is double-edged. On the one hand, it provides users with more personalized and efficient information services; on the other hand, it may create information silos, limit users' access to information channels, and even be used to manipulate users' decisions and views. Therefore, while enjoying the conveniences brought by targeted delivery, we should strengthen data security protection to ensure that user privacy is not violated. At the same time, conducting in-depth research and regulation on the impact of targeted delivery is necessary to protect users from undue influence and ensure the diversity and fairness of information.

2. The Facebook Data Breach Incident

The Facebook data breach incident originated from the Strategic Communication Laboratories Group (SCL), a consulting firm based in the UK that specializes in strategic communication and psychological warfare. Since its establishment in 1990, SCL has included several branches such as Cambridge Analytica, serving governments, military organizations, businesses, and political candidates. The company has provided psychological consulting for the US and UK military during the wars in Afghanistan and Iraq, aiming to influence the battlefield through psychological means, such as persuading children not to join terrorist organizations or encouraging villages to surrender. Through its operations, SCL discovered that its theories and methods had broader applications─elections. Confessore (2018, pp.4, 1-9) found that every country has elections with numerous participants and significant funding, presenting a vast business opportunity for SCL. Thus, SCL engaged in elections around the world as political consultants, including the 2015 Argentine election, the 1997 Thai election, the 2009 Trinidad and Tobago election, the 2010 Indian general election, and the 2013 Malaysian general election (Rosenberg et al., 2018). It was not until 2013 that a paper published by Michal Kosinski, David Stillwell, and Thore Graepel from Cambridge University, titled "Private traits and attributes are predictable from digital records of human behavior," revealed the possibility of predicting personal traits by analyzing behavior records on Facebook (such as likes, shares, and comments), marking the beginning of SCL's involvement in political consulting using big data technology (Kosinski et al., 2013).

The research team used machine learning models to analyze a vast amount of Facebook users' "like" data, combined with the results of psychological tests. Kosinski et al. (2013) recommended that the results showed that merely based on "like" behavior, it was possible to accurately predict users' sexual orientation, political leanings, religious beliefs, age, gender, intelligence, and drug use among other personal traits. SCL was particularly interested in this research, especially the method of data acquisition. Kosinski et al. (2013) recommended that the research team conducted surveys on Facebook through third-party apps, claiming research purposes to collect user data, accumulating data from 58,000 people over six years. SCL realized that by utilizing the data from Facebook, which covers a wide range of countries and has billions of online users, it could precisely understand each person's personality and political leanings. Combined with SCL's years of psychological warfare techniques, it was sufficient to influence national elections. Therefore, SCL established Cambridge Analytica in the UK, borrowing the name of Cambridge University where the authors of the paper were based (hereafter referred to as CA in the article) (Christian et al., 2021).

The Facebook data breach incident evolved into version 2.0 with Cambridge Analytica's election manipulation process divided into three steps: data acquisition, data analysis, and behavior modification. Initially, CA intended to acquire data through funding and contacted researcher David Stillwell, hoping to utilize the Facebook interface he researched. However, Stillwell refused CA due to the realization of the illegal use of the data. Subsequently, CA turned to another Cambridge University researcher, Aleksandr Kogan. Drawing on Stillwell's method, Kogan developed a new app called "This Is Your Digital Life," which posted a 120-question survey on Facebook, offering a compensation of $2-4 per survey. During the data collection process, Kogan discovered and exploited a loophole in Facebook, allowing the collection of participant data and their friends' data (Tadese et al., 2018). Utilizing this loophole, 270,000 surveys were distributed within a few months, ultimately collecting data from over 50 million users. CA claimed to have obtained data on all eligible voters in the US, leading to the most extensive data breach in history.

Once CA obtains the user data, data analysis can be performed easily. CA used a five-dimensional personality analysis method called OCEAN (As Showed in Figure 1) to analyze individual personality traits (Ackerman, 2019). OCEAN is an acronym for the five personality dimensions: Openness to experience, Conscientiousness, Extraversion, Agreeableness, and Neuroticism. Individuals high in Openness are open to new experiences, curious, and creative; those high in Conscientiousness are disciplined, well-planned, and detail-oriented; individuals high in Extraversion are sociable, confident, and active; those high in Agreeableness are friendly, cooperative, and caring towards others; individuals high in Neuroticism experience large emotional fluctuations and are easily stressed.

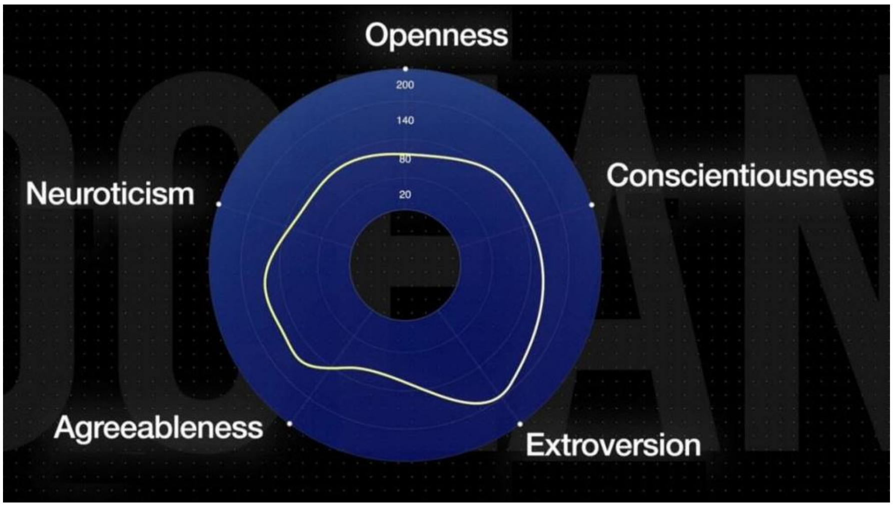


Figure 1: Schematic diagram of the OCEAN analysis method

Cambridge Analytica (CA) Company utilized the five-dimensional personality analysis method to infer individual personality traits based on user behavior data (such as likes, shares, comments) on social media and other digital platforms (Martin, n.d.). This approach enabled the company to gain a deeper understanding of individuals' psychological and behavioral tendencies, thereby formulating personalized marketing and political propaganda strategies to achieve precise target positioning and enhance the impact. At a press conference, the head of CA confidently claimed the ability to accurately predict the personality of every adult American. Although the statement was boastful, it also reflected the vast amount of data the company had mastered. By applying the five-dimensional personality analysis, CA completed the second step of data analysis.

After extensive preparation, CA joined the US election, becoming part of the Trump campaign team (Investopedia, 2019). CA's main task was to use its expertise in behavior change technology to influence the election outcome. Why did CA excel in this field? Take the "Do So" campaign by SCL Company (CA's parent company) in the Trinidad and Tobago election as an example. This campaign was a psychological operation strategy aimed at weakening the opponent's support base by encouraging young voters not to vote (Figure 2 shows some promotional activities of the "Do So" campaign). SCL deeply analyzed the target group and used marketing and communication strategies to promote the "Do So" message through multiple channels such as social media, advertising, and public events. This strategy appeared to be a grassroots social movement but actually leveraged young people's disappointment and dissatisfaction with politics, encouraging them to express their protest by not voting. The politics of Trinidad and Tobago are divided into religious and secular factions. SCL's strategy cleverly influenced the secular faction through neutral activities, while the religious faction was less affected due to family and religious ties. The results showed that in the 18-35 age group, the religious faction reversed 35% of the vote, winning unexpectedly. SCL's strategy successfully influenced voting behavior, achieving the client's goal.

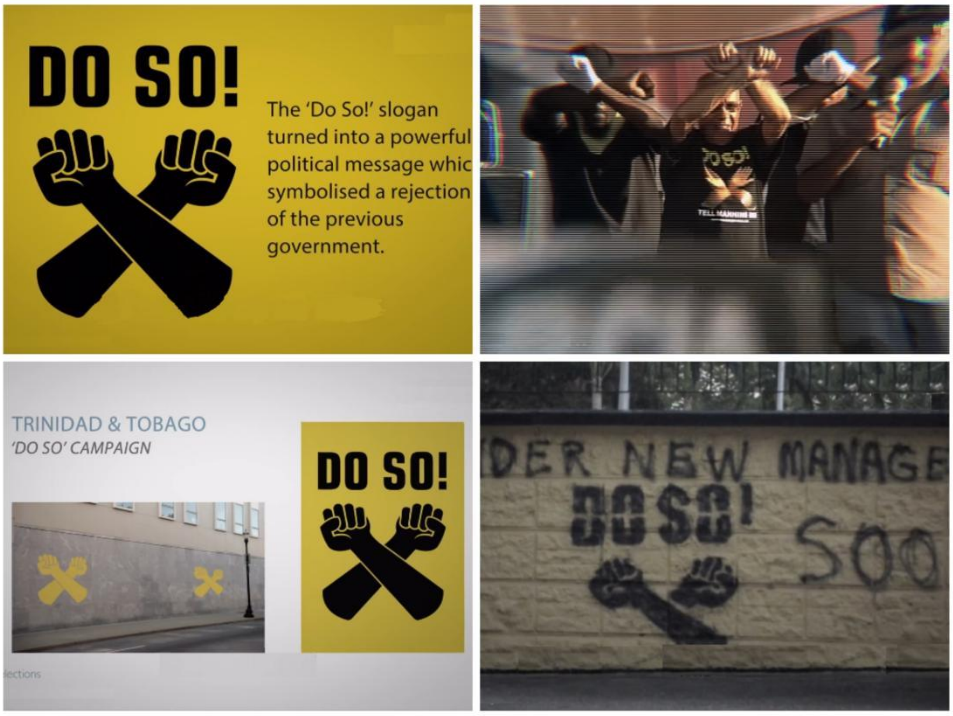

DO SO!
The 'Do So!' slogan turned into a powerful political message whic symbolised a rejection of the previous government.
DO SO!
TRINIDAD & TOBAGO
'DO SO' CAMPAIGN
DO SO!
lections
DER NEW MANAGE
DO SO!
SOO

Figure 2: Part of the promotion behavior of the "Do So" activity

During Donald Trump's 2016 presidential campaign, Cambridge Analytica (CA) utilized big data and precision targeting technology, adopting a strategy known as "Micro targeting." This strategy, through detailed data analysis and psychological profiling, precisely targeted specific voter groups and sent them personalized messages to influence their voting decisions. The core involved using big data and psychological models (such as the OCEAN five-dimensional personality model) to construct psychological profiles of voters. CA analyzed a vast amount of personal data (such as social media activity, online behavior, purchase history, etc.), identifying voters' personalities, interests, and political leanings. Based on this information, CA segmented voters into groups with specific characteristics and preferences, designing customized messages and advertisements for each group aimed at touching emotions and influencing perceptions of Trump or other candidates (Tappin, B. M., Wittenberg, C., Hewitt, L., Berinsky, A., & Rand, D. G., 2023). For example, for anxious voters leaning towards Hillary, advertisements that incited panic, such as "Without Trump, America will be destroyed," were pushed. For voters who valued family, advertisements highlighting Trump's focus on family income and community building were pushed. If data showed a group was concerned about gun control, messages emphasizing Trump's support for gun rights were pushed. This strategy aimed to stimulate support or at least influence opponents' views, making the Trump team's campaign funding more effective and maximizing impact. Despite most websites predicting only a 15% chance of Trump winning, he ultimately won by a narrow margin. According to insiders at Facebook, Trump's advertisements on social media far outperformed Hillary's, with CA playing an indispensable role.

Until 2018, the Facebook data breach became widely known through in-depth media reports and a whistleblower from Cambridge Analytica (CA). This incident led to a widespread data leak, resulting in multiple consequences:

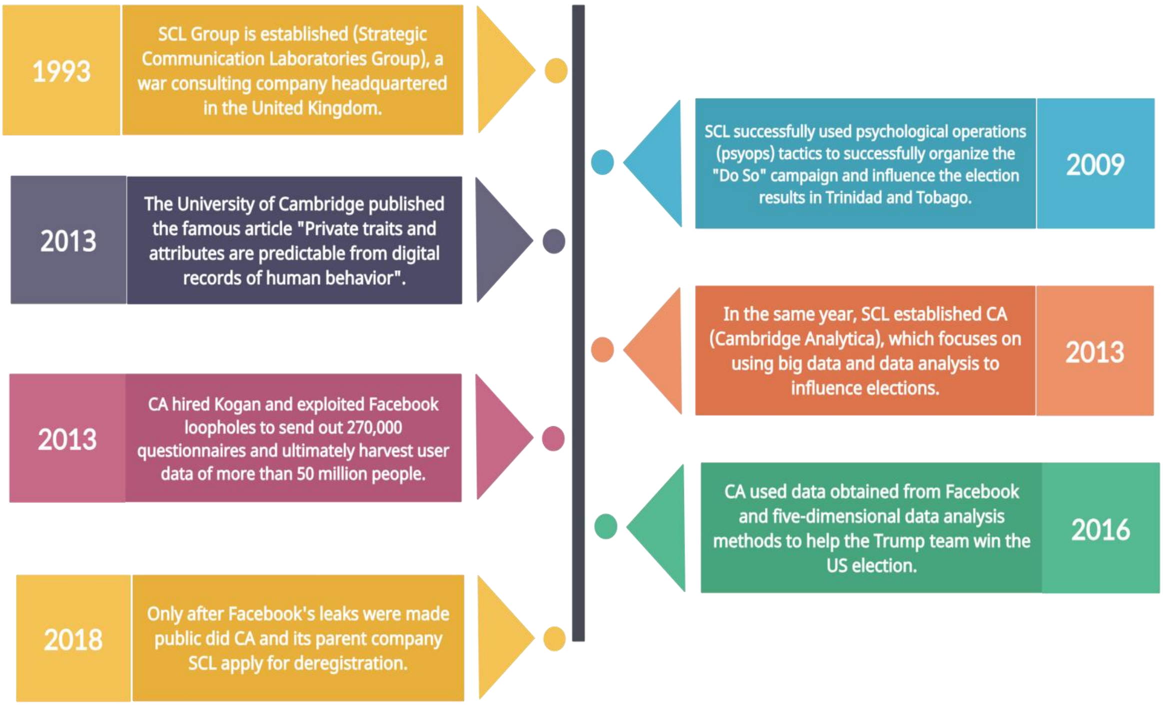
1) Public Trust Decline: This incident severely damaged the public's trust in Facebook and other major tech companies regarding the handling of personal data. Users became seriously concerned about the collection, use, and protection of their personal data. Following the outbreak, Facebook's stock price plummeted by 24%, erasing nearly $120 billion in market value, setting a record for the largest market value shrinkage in history. Investors expressed strong dissatisfaction with Facebook's mistakes in data security and privacy protection.

2) Increased Regulation: The data breach intensified criticism of insufficient regulation of tech giants. Regulatory bodies in the United States, the United Kingdom, the European Union, and other regions began investigating Facebook and planned to strengthen the regulation of internet companies in terms of data security and privacy protection. This incident prompted governments and regulatory agencies worldwide to tighten regulations on tech companies. Against this backdrop, the European Union's General Data Protection Regulation (GDPR) received more attention, establishing stricter rules for personal data protection.

3) Facebook Policy Reform: After the incident, Facebook announced a series of reform measures, including restricting third-party apps' access to user data, increasing data usage transparency, and enhancing account security measures, aiming to rebuild user trust. To reshape user trust, tech giants like Facebook were forced to strengthen internal privacy protection management and proactively accept external supervision and audits. Confessore (2018) recommended the industry's self-discipline awareness was enhanced.

4) Data Awareness Awakening: This incident made the public realize that in the digital age, their inadvertently generated digital footprints could be misused, harming the public interest. Consequently, data protection awareness rapidly increased. Confessore (2018) recommended this event heightened public awareness of personal data privacy and information security, prompting users to share personal information more cautiously and to scrutinize the online services and applications they use more rigorously.

Ultimately, under external pressure, CA and its parent company SCL applied for dissolution in 2018, marking the end of the Facebook data breach incident. Reviewing this event, it is clear that although CA violated laws and management regulations by illegally obtaining data through exploiting Facebook's vulnerabilities, their use of big data analysis and precision targeting strategies was indeed effective. Moreover, there were rumors that CA was involved in the Brexit referendum, unexpectedly influencing the outcome. This article presents the entire process of the Facebook data breach incident through a timeline diagram (Figure 3).



1993 SCL Group is established (Strategic Communication Laboratories Group), a war consulting company headquartered in the United Kingdom.

2009 SCL successfully used psychological operations (psyops) tactics to successfully organize the "Do So" campaign and influence the election results in Trinidad and Tobago.

2013 The University of Cambridge published the famous article "Private traits and attributes are predictable from digital records of human behavior".

2013 In the same year, SCL established CA (Cambridge Analytica), which focuses on using big data and data analysis to influence elections.

2013 CA hired Kogan and exploited Facebook loopholes to send out 270,000 questionnaires and ultimately harvest user data of more than 50 million people.

2016 CA used data obtained from Facebook and five-dimensional data analysis methods to help the Trump team win the US election.

2018 Only after Facebook's leaks were made public did CA and its parent company SCL apply for deregistration.

Figure 3: Timeline map of Facebook leaks

3. Understanding Precision Targeting From The Facebook Leak Incident

Precision targeting is a marketing approach that leverages big data analysis and artificial intelligence algorithms to provide users with personalized information and services. It primarily utilizes data analysis techniques and machine learning algorithms to deeply mine and analyze user data, understanding users' behavior patterns, preferences, and needs to achieve personalized content customization and precise delivery. The core ideas of precision targeting include:

1) Data Collection: Using web crawlers, user browsing records, mobile device sensors, and other means to collect users' digital footprints and behavioral data. For instance, in the Facebook data breach incident, Cambridge Analytica collected data in this manner.

2) User Profiling: Through big data analysis and machine learning technologies, a comprehensive analysis of users' demographic attributes, interests, consumption habits, and social relationships is conducted to build detailed user profile models. This process was exemplified in the Facebook data breach incident where Cambridge Analytica classified voters using a five-dimensional personality analysis method.

3) Personalized Content Generation: Customizing personalized content that matches the preferences and needs of different user groups, including product promotions, news, entertainment videos, etc.

4) Algorithmic Matching and Delivery: Employing artificial intelligence algorithms, combined with user profiles and contextual scenarios, to predict which content is most appealing to specific users, thereby achieving efficient and precise content delivery (Bose & Mahanti, 2022, pp.16(2), Article 12).

5) Automatic Optimization and Iteration: Automatically adjusting delivery strategies based on user feedback on the content, continuously optimizing content and timing of delivery to improve precision and conversion rates (Xu et al., 2023, pp.14(1),23-45).

The advantage of precision targeting lies in its ability to meet users' real needs to the greatest extent, providing a highly personalized and humanized service experience, avoiding the interference of ineffective advertisements, and significantly improving the precision and conversion outcomes of marketing. As an important strategy in modern digital marketing, precision targeting greatly enhances the effectiveness and efficiency of marketing activities through the application of big data and artificial intelligence technologies. Based on the analysis of the characteristics of precision targeting, we recognize that as a personalized marketing method relying on big data analysis and artificial intelligence algorithms, precision targeting mainly has the following advantages:

1) Precision and Efficiency in Marketing Deployment: Compared to traditional marketing, precision targeting, through detailed user profile analysis, can accurately identify target user groups with high interest and purchasing intent, significantly reducing advertisement waste and enhancing the efficiency of marketing resource utilization.

2) Humanized User Experience: Precision targeting can accurately predict users' interests and needs, providing information that matches individual preferences, reducing the interference of spam advertisements, offering a more considerate and high-quality service experience, and enhancing users' goodwill towards the brand.

3) Bose & Mahanti (2022, pp.16(2), Article 12) recommended growth in Conversion Rates and Revenue: Due to the highly personalized and contextualized content of precision targeting, it is more likely to attract users, naturally increasing click-through rates and conversion rates, positively impacting corporate revenue and profits.

4) Xu et al. (2023, pp.14(1),23-45) recommended Immediacy and Directness of Feedback Data: In the process of precision targeting, the feedback on personalized content from users is immediate and direct, allowing companies to quickly capture users' real preferences and adjust marketing strategies in a timely manner, forming a virtuous cycle.

5) Scientific Nature of the Overall Strategy: Relying on big data and AI algorithms, precision targeting makes marketing strategies more scientific, systematic, and forward-looking, avoiding the blindness led by traditional experience and introducing a new technological paradigm to marketing.

6) In-depth User Research: Precision targeting requires comprehensive and detailed analysis of users, which in turn deepens enterprises' understanding of their target audience, providing valuable insights for product and service optimization.

Overall, precision targeting is an important trend in marketing in the era of big data, significantly promoting the improvement of marketing precision and conversion rates, optimizing user experience, and enhancing brand competitiveness. However, with the excessive mining and utilization of personal data, issues of privacy infringement and algorithm manipulation have raised widespread concern. How to protect users' rights and public interest while achieving precision targeting, maintaining social fairness and justice, becomes a significant issue that needs to be addressed (Wang, 2019, pp.4(2), 1-15).

4. Conclusion

The Facebook data breach incident was a significant data security event that affected at least 50 million users, involving the leakage of personal information such as names, birthdays, locations, interests, and relationship statuses. As a result, Facebook faced legal and regulatory scrutiny, with the Federal Trade Commission (FTC) imposing a fine of $5 billion on it and demanding improvements in privacy protection measures. This incident has drawn widespread public attention to personal data privacy and the responsibility of social media platforms, prompting Facebook to take measures to strengthen data security, including changing privacy settings and restricting third-party app access permissions. This not only exposed the flaws of social media in data protection but also promoted a profound reflection on digital privacy, data security, and social media regulation globally.

In today's era of big data, the collection and analysis of personal information have become an indispensable part of corporate marketing strategies. The Facebook data breach incident, as a typical case, provides us with an opportunity to delve into the application of big data and its potential risks. This article aims to reveal, through a detailed analysis of the Facebook incident, how companies utilize user data for precision targeting in the context of big data, as well as the basic principles and technical means followed in this process. Firstly, this article will introduce the basic concepts and technical framework of precision targeting, including key links such as data collection, analysis, and application. Subsequently, through a case analysis of the Facebook data breach incident, this article will show how companies apply these technical means in practice and the privacy leakage and data security issues that this application may bring. The Facebook incident has not only raised global attention to personal data privacy and security but also prompted governments and regulatory agencies worldwide to re-examine data protection regulations and policies. For example, the U.S. government's scrutiny and demands on TikTok are precisely out of consideration for national security and personal privacy protection (Sanger, 2020). This move not only reflects the importance of personal data privacy and security on the international stage but also marks an increase in data regulation awareness globally. However, as an effective marketing tool, the advantages of precision targeting in improving marketing efficiency and optimizing user experience cannot be ignored (Shi, 2023, pp.23(1), 26-45). Therefore, how to reasonably utilize precision targeting technology under the premise of protecting personal privacy and data security has become an urgent problem to be solved. This article will explore how enterprises, governments, and individuals can work together under the current technological and legal framework to find a balance point that can fully leverage the advantages of big data while effectively protecting personal privacy and data security. Finally, this article will propose several suggestions, including strengthening data protection regulations, raising public awareness of data security, corporate self-regulation, and technological innovation, aiming to provide references for solving the regulatory challenges brought by precision targeting. Through these measures, we hope to promote a safer and more transparent big data application environment, protect personal privacy, and also safeguard the legitimate rights and interests of enterprises and users.

Acknowledgement
The authors would like to express their appreciation and gratitude to the Universiti Teknologi MARA for funding this publication.

References

Ackerman, C. E. (2019). Big Five Personality Traits: The OCEAN Model Explained. Positive Psychology. Retrieved from https://positivepsychology.com/big-five-personality-theory/

Bose, R., & Mahanti, A. (2022). Algorithmic Matching and Delivery in Precision Targeting. ACM Transactions on the Web, 16(2), Article 12.

Chandra, S. (2022). Personalization in personalized marketing: Trends and ways forward. Psychology & Marketing, 39(4), 10.1002/mar.21670. https://doi.org/10.1002/mar.21670

Christian, H., Suhartono, D., Chowanda, A., et al. (2021). Text based personality prediction from multiple social media data sources using pre-trained language model and model averaging. Journal of Big Data, 8, 68. https://doi.org/10.1186/s40537-021-00459-1

Confessore, N. (2018). Cambridge Analytica and Facebook: The scandal and the fallout so far. The New York Times, 4(2018), 1-9.

Investopedia. (2019). Cambridge Analytica: Overview, History, Example. Retrieved from Investopedia website

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences, 5802‑5805. https://doi.org/10.1073/pnas.1218772110

Martin, C. (n.d.). The Big Five OCEAN Personality Types: Introduction and Discussions. Retrieved from https://blog.flexmr.net/ocean-personality-types

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018). How Trump consultants exploited the Facebook data of millions. The New York Times, 17, 2018.

Sanger, D. E. (2020). U.S. Says TikTok Needs to Be Sold or Face a Ban. The New York Times. Retrievedfrom https://www.nytimes.com/2020/08/03/technology/tiktok-ban-sale-trump.html

Shi, Y. (2023). Precision advertising and optimisation strategy based on big data algorithms. International Journal of Information Technology and Management, 23(1), 26-45. https://doi.org/10.1504/IJITM.2023.131806

Sivarajah, U., Irani, Z., Gupta, S., & Mahroof, K. (2020). Role of big data and social media analytics for business to business sustainability: A participatory web context. Industrial Marketing Management, 163‑179. https://doi.org/10.1016/j.indmarman.2019.04.005

Tariq, M. U. (2021). Human Behavior Analysis Using Intelligent Big Data Analytics. Frontiers in Psychology, 12.

Tadese, M. M., Lin, H., Xu, B., & Yang, L. (2018). Personality predictions based on user behavior on the Facebook social media platform. IEEE Access, 6, 61959-61969. https://doi.org/10.1109/ACCESS.2018.2876502

Tappin, B. M., Wittenberg, C., Hewitt, L., Berinsky, A., & Rand, D. G. (2022). Quantifying the Potential Persuasive Returns to Political Microtargeting. https://doi.org/10.31234/osf.io/dhg6k

Voigt, P., & Von dem Bussche, A. (2017). The EU general data protection regulation (GDPR): A practical guide. Springer Nature.

Wang, Y. (2019). Data Mining and Privacy Protection: Challenges and Opportunities. Journal of Data and Information Science, 4(2), 1-15.

Xiao, C. (2019). Personal Data Rights in the Era of Big Data. Social Sciences in China, 40(3), 45-52. https://doi.org/10.1080/02529203.2019.1639962

Xu, L., et al. (2023). Automatic Optimization and Iteration in Precision Targeting Strategies. Data & Information Management, 14(1), 23-45.

Zongyu Song. (2022). Systematic Regulation of Personal Information Rights in the Era of Big Data. Journal of Intelligence, (12), 158.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Public Affairs.