The Impact of AI-Driven Personalization Tools on Privacy Concerns and Consumer Trust in E-commerce

Auteur : Amil, Yasmine
Promoteur(s) : El Midaoui, Youssra
Faculté : HEC-Ecole de gestion de l'Université de Liège
Diplôme : Master en sciences de gestion, à finalité spécialisée en international strategic marketing
Année académique : 2023-2024
URI/URL : http://hdl.handle.net/2268.2/21371

The Impact of AI-Driven Personalization Tools on Privacy Concerns and Consumer Trust in E-commerce

Jury :

Supervisor:

Ms. Youssra El Midaoui

Reader:

M. Willem Standaert

Master thesis by

Yasmine Amil

For a master in

« International Strategic Marketing »

Academic year 2023/2024

ABSTRACT

The incorporation of AI (Artificial Intelligence) tools in e-commerce has brought about significant benefits and challenges for businesses and customers. AI technologies have provided personalization tools for business to tailor their product experiences according to individual customer needs, which has helped businesses create customer loyalty and satisfaction. On the other hand, the incorporation of these AI-driven personalization tools in business has also raised critical privacy concerns. This is attributed to the heavy reliance on data of these AI-driven personalization tools. Therefore, this research study seeks to investigate the impact of AI-driven personalization tools on privacy concerns within the e-commerce sector. Furthermore, the research study seeks to evaluate how these privacy concerns on AI-powered recommendation systems influence users' trust in the competence of the AI system and the trust in the Alignment of the AI system with their ethical values. To achieve these objectives, the researcher uses a quantitative research design. The researcher administered a survey to 453 respondents, including Amazon customers and reviewers. The tool used for data collection is the Lime Survey. The researcher conducted data analysis using SPSS statistical data analysis tools. The data analysis was meant to test hypotheses and identify relationships between the research variables. The findings of the research study reveal that high perceived benefits of personalization decrease a user's privacy concerns about an AI system. However, the perceived anonymity of the internet did not yield significant results. On the other hand, the findings of the research study reveal that high perceived risks (data breach risk and consent risks) increase the privacy concerns of users.

ACKNOWLEDGEMENTS

First, I'd like to convey my heartfelt gratitude to my supervisor, Youssra El Midaoui, for her constant direction, invaluable insights, and ongoing mental and academic support throughout the study. Your effort and guidance helped shape the structure of this thesis. At the same time, I would like to sincerely thank Dr. Willem STANDAERT, thank you for agreeing to be the reader of my thesis. Thank you for your interest and your time. I want to acknowledge the valuable contributions of all the individuals, resources, and references that have played a role in shaping the foundation of this thesis. Each piece has contributed to the overall knowledge that this work embodies. Last but not least, thanks to: My dear mother, for accompanying me with her soul and heart on a difficult path, for healing my wounds and being a balm for the soul and body, for being a compassionate heart and a warm hug. My father and brother, who protected me from life's incidents and to the heroes of my story. To my friend and companion, to the one who wrote my novel with me, to the one who understands me without speaking.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

1 INTRODUCTION

1.1 Background and Context

In recent years, the rapid advancement of technology has significantly transformed E-commerce. A key innovation that has revolutionised E-commerce is the integration of AI-driven personalisation tools. The increasingly competitive landscape of E-commerce has led to the significant growth of the adoption of AI in business as many businesses have adopted AI into their E-commerce platforms (Khrais, 2020). The article by Joshua, (2023) states that by the year 2020, 78% of E-commerce brands globally had incorporated AI into their operations. The report highlights that AI in E-commerce is continuously growing, and by the year 2030, AI-based revenue in E-commerce is expected to reach $16.8 Billion.

To function effectively, AI-driven personalisation heavily relies on data (Castillo & Taherdoost, 2023). These AI technologies enable the collection, storage, and processing of vast amounts of data. The data is thereafter used to deliver personalised experiences to the users. E-commerce platforms use AI technologies in the form of machine learning, predictive analytics, and natural language processing to analyse vast amounts of customer data and provide personalisation to E-commerce platforms whereby products and services are tailored to an individual's consumer preferences (Cheng et al., 2023). AI technologies create a more engaging shopping experience that feels tailored to the individual. When customers feel that a platform understands their needs, they are more likely to spend more time on the site and engage with the platform. This implies that AI technologies play a crucial role in boosting customer engagement levels. This enhances the likelihood of purchase as well as repeat purchases, as customers may tend to be loyal to a platform that meets their customer needs. It is important to note that AI-driven personalisation tools play a crucial role in enhancing company sales.

While these technologies have been pivotal in increasing conversion rates of E-commerce platforms by personalising customers' shopping experiences, the heavy reliance on data has raised significant privacy issues among customers. Many people have been increasingly concerned about how their data is used and the potential risks involved when someone misuses their data. These concerns have led to a growing debate on the balance between personalization benefits and the protection of consumer privacy. Therefore, this research study seeks to investigate the impact of AI-driven personalization tools on privacy concerns and consumer trust within the e-commerce sector.

1.2 Motivation

Personalization has gained popularity as a tactic in e-commerce to enhance the purchasing experience for customers. It has the ability to provide the appropriate product to the appropriate person at the appropriate moment in the appropriate context (Raji et al., 2024). Specifically, platforms now have access to increasingly complex AI-driven personalization tools that can exploit and make sense of the unique conclusions derived from the mass user data thanks to the growth of big data and AI technology (Ma & Sun, 2020). Consumer trust and privacy issues are significantly impacted by these personalization capabilities (Lina and Setiyanto, 2021).

Retailers have adopted AI-driven personalization tools, but e-commerce has generated a lot of client data, putting their privacy in danger (Holmström & Larsson, 2024). Because advanced personalization tools rely on users' willingness to divulge personal information beyond what is strictly required to complete an online transaction, sellers and buyers are growing more concerned about the privacy costs associated with them (Maseeh et al., 2021). Numerous studies have demonstrated how general privacy concerns can result in unfavorable opinions about data usage and, as a result, build a barrier that restricts the useful applications of online shops, thus reducing their sales (Maseeh et al., 2021).

This research intends to investigate how sophisticated AI-driven personalization tools in e-commerce affect consumers' trust in retailers and privacy concerns in light of these gaps in the literature (Maseeh and others, 2021).

1.3 Problem Statement

Many companies have incorporated AI-driven personalisation tools into their E-commerce platforms. These new technologies have created both significant opportunities and challenges. These tools have played a crucial role in tailoring a company's products and services to the needs of their individual customers, which has played a central role in creating higher engagement levels and increased customer satisfaction. On the other hand, the reliance of these technologies on vast amounts of personal data has raised critical concerns regarding customer privacy and trust.

The integration of AI-driven personalisation tools into E-commerce platforms has exposed customers to various types of data-related risks. One of the common risks of loss of data in E-commerce platforms is financial fraud. Financial fraud in e-commerce platforms occurs when

cybercriminals exploit customer data on credit card numbers, bank account details, and payment histories. As a result of this, Consumers face the risk of monetary loss through fraudulent transactions facilitated by compromised payment information. In fear of such events, customers have been increasingly wary of how their data is collected, stored, and shared.

The core of the problem lies in the balance between the benefits of AI-driven personalization and the potential risks associated with data privacy. The research study seeks to address this by analysing how to explore the impact of AI-driven personalization tools on privacy concerns and how these concerns, in turn, affect consumer trust. By understanding these dynamics, the study will provide insights into how e-commerce platforms can optimize their use of AI technologies while maintaining consumer trust.

1.4 Contribution

This research makes several key contributions to the understanding of AI driven personalization in E-commerce and its impact on customer's privacy concerns and trust. The research study gives a comprehensive analysis of the benefits as well as the risks associated with the use of AI technologies in E-commerce. Therefore, it creates a nuanced understanding of the challenges experienced by e-commerce platforms brought by the incorporation of AI personalization technologies. The findings of this research study will be beneficial to E-commerce businesses as they will provide insight into how to balance the benefits of AI-driven personalization with the need for data protection. The research sheds light on factors that contribute to consumer apprehensions about data privacy, providing valuable insights into the ways in which these concerns influence consumer behaviour. In addition, the findings of this research study will be beneficial to policymakers in creating frameworks that balance innovation and consumer protection from loss of data to unauthorised parties. Furthermore, the findings of this research study will contribute to the growing body of literature on AI, e-commerce, and data privacy by offering an empirical analysis of the relationship between personalization technologies and consumer trust. Furthermore, this research study provides additional insight into the impact of AI usage on two different dimensions of consumer trust in AI, which are Trust in AI competence and Trust in AI alignment.

1.5 Approach

The thesis begins with an analysis of the background and context of the research study and analysis of the problem statement. Thereafter, the researcher proceeds to the Literature review Section. In this section, the researcher uses relevant search terms to screen previous research materials that relate to this area of study. Thereafter, the researcher analyses the different perspectives of these research studies on AI-driven personalization, privacy concerns, and consumer trust within the e-commerce sector. The researcher uses the Privacy calculus theory as the theoretical framework for the research study. This is later used to build a conceptual framework that guides the study's approach to understanding the relationship between AI technologies and privacy concerns. Thereafter, the methodology section outlines the research design, which employs a quantitative research tool to gather data from a sample of Amazon reviewers. Thereafter, the results section analyses both descriptive (insights into demographic factors) and inferential (insights into variable relationships) statistics. Thereafter, relevant discussions are made concerning the results. The final chapter provides the conclusions, limitations of the research study, and relevant recommendations.

2 LITERATURE REVIEW

2.1 AI Recommendation systems in E-commerce

Kumar et al., (2019) defines AI as machines that can think and perform like human beings. AI-assisted technology can mimic the functions of the human mind, also their ability to solve problems and learn things. As a result, AI could acquire, process, and identify data before performing specific tasks (Jarek and Mazurek, 2019). Alternatively, to describe it a different way, artificial intelligence (AI) is the technology that enables machines to act like humans and learn from their experiences (Davenport et al., 2020).

Specifically, integration of AI in E-commerce entails using of AI assisted tools, systems and algorithms that support the buying and selling of products over the Internet (Soni, 2020). One of the key applications of AI in E-commerce is empowering customer relationships through personalisation. AI-enabled personalised interactions with the customer, use data driven techniques to tailor the shopping experience to specific needs and preferences of a customer (Todor, R. (2017). However, it is important to note that personalisation's reliance on user data for customisation presents an issue of consumer privacy (Jones, 2019). The accumulation of personalised data by AI tools poses a risk of unauthorised access which may eventually compromise an individual's privacy.

E-commerce businesses frequently seek to increase their sales by improving sales conversion rates. Unlike the traditional e-commerce business, whereby Customers' personal data is underutilized, AI technologies, specifically machine learning algorithms, enable e-commerce businesses to collect customer’s personal data and better understand customer habits, intentions, and preferences, leading to improved shopping experiences, and improved sales conversion (Yin & Qiu, 2021). The AI personalisation tool adopts the offline sales model where a sales representative meets with customers and recommends products. In this case, the recommendations are digitalised, allowing for the provision of multiple products based on customer demand model (Shankar et al. (2021). One of the features that facilitates the AI driven product recommendation model is the K-NN (K-Nearest Neighbor) Algorithm. This is a machine learning approach utilised to enhance various aspects of the online shopping experience, particularly in product recommendation systems. E-commerce platforms often employ K-NN algorithms to suggest products to customers based on their similarities to other

users (Yasin et al., 2023). By analysing historical data, the algorithm identifies products that are frequently bought together or are similar in features and recommends them to users who have shown interest in similar items (de et al.2021).

Additionally, another technique that companies use to understand consumer behaviour is sequence mining. Companies can use sequence mining to analyse customer navigational patterns when they start a website session, make active clicks, and add products to their shopping cart (Requena et al. 2020). Identifying and categorising key products in frequent navigation sequences can help identify and cluster customer preferences (Satheesan et al. 2020). The products in the cluster that contain the product that the customer first browses are recommended as associated products. Improving performance requires sophisticated algorithms and effective machine learning solutions (Wang et al.2020). Algorithm-based solutions typically involve three stages: collecting and filtering data, grouping customers based on navigational patterns, and selecting effective online buddies to present recommendations (Ko et al., 2022). Mishra and Tyagi (2022) suggest that incorporating cloud-based machine learning and data analytics can enhance productivity in online businesses and benefit any commercial or trading company. In consequence, session-based personalized product recommenders indeed improve online shopping experiences and increase e-commerce conversion rates (Lo et al.2021).

Basically, AI Recommendation System function as a personal and social adviser, advising users based on their needs and personality (Dey, 2021). It gathers information about the user's likes and dislikes, then filters products based on those preferences (Rashidin et al., 2021). Such recommendation systems are widely used by e-commerce giants such as eBay and Amazon to improve business intelligence, understand customer preferences, and develop smart business strategies (Al-Qudah et al., 2023).

2.2 Comprehensive Approaches and Applications in AI Recommendation Systems

AI powered domains use structured approaches to devise and implement personalised recommendation strategies, which include four major components: equipment filtering, collaborative filtering, content-based filtering, and hybrids (Gunasekar et al., 2023). First and foremost, equipment filtering entails recommending items based on specific item attributes. It focuses on matching user preferences with specific item attributes. Secondly, Content-based filtering recommends items to users based on the actual content of the items themselves

(Javed et al.2021). It entails analysing item attributes and content and matching them with user preference. On the other hand, collaborative filtering identifies similarities between users and leverages this information to suggest items that similar users have liked. Additionally, the hybrid model combines the capabilities of collaborative and content-based filtering to increase user satisfaction. Despite their usefulness, there is a gap in theoretical evaluations of these hybrid models, indicating a potential subject for future research. This review will look into various methodologies, with a special emphasis on the ability of hybrid approaches to overcome the constraints of traditional methods.

In general, the primary goal of this systems is to increase product sales by providing customers with relevant items, thereby increasing total profit. This goal incorporates the functional goals of recommendation systems, such as diversity, serendipity, and relevancy, with the goal of improving the online shopping experience by providing personalised and relevant product recommendations (Vivek, Manju, and Vijay, 2018). These systems are becoming increasingly popular among online shoppers due to their effectiveness and simplicity, as they provide an alternative to manual search by predicting user preferences based on their interests, needs, and preferences and comparing them to those of other user groups. Recommendation systems are utilised in a variety of contexts, such as advising on clothing purchases, friend-matching preferences, and online news consumption. Also, based on data taken from a user profile or an item's ratings, they provide suggestions. Among the key technologies enabling the creation of intelligent clothing suggestion systems and smart shopping devices are artificial intelligence, machine learning, deep learning, and computer vision. Clothing recommendations have a special function in that they not only recommend related products to fit users' existing dressing preferences, but they also offer customised styling advice to assist users better grasp customised styling (Nikzad-Khasmakhi, Balafar, & Feizi-Derakhshi, 2019).

These recommendation systems do not simply provide suggestions but they make it easier to choose from a wide range of products that hold the same level of preference or positioning in the customer's mind (Kuc¸¨ ukbay & Turhan, 2019). Artificial intelligence (AI), particularly computational intelligence and machine learning techniques and algorithms, has been applied in the process of developing recommender systems to address issues with cold start and lack of data by increasing forecast accuracy (Zhang, Lu, & Jin, 2021). In order to show the intelligence of such systems, when a viewer wants to select the next item, the company's

system evaluates viewer preferences and provide recommendations (MADEN BİLGİÇ, 2022). Those intelligent systems can plan, reason, learn, and adapt, providing guidance based on prior knowledge and assisting in complex decision-making processes (Lari et al., 2022). They significantly reduce the likelihood of human error, increasing efficiency and effectiveness across multiple domains.

Additionally, Shahid and Li, (2019), states that application of AI in marketing plays a central role in improving information understanding, conversion rates and customer happiness. This is supported by Chintalapati and Pandey (2022), who believes that AI integrates with marketing strategies to strongly improve buyer engagement. So Predictive analytics really helps marketers forecast customer behavior and trends, leading to better purchases, upsell opportunities, and overall customer experience (Zhang et al., 2021). Making data-driven judgments and improving strategies for marketing are both possible with these insights. These systems identify detailed patterns of interests and actions, and make personalised recommendations (Zhang et al., 2021; Sarker, 2021). This can not only improves product classification but also the efficiency of product suggestions, allowing clients to find what they accurately need and desire more quickly (Lee & Shin, 2020; Wang et al., 2020). In summary, marketing experts believe that personalisation across all marketing channels is critical to success in today's e-commerce landscape, with AI-driven personalisation expected to shift from explicit to implicit, predicting client desires before they are even aware of them (Renjith et al.2020; Alamdari et al.2020).

One of the ways that marketers use to enhance their marketing strategies in the Internet is Search engine Optimisation and Pay Per Click campaigns. SEO involves optimising website content to improve organic search engine rankings, while PPC involves placing ads on search engines and paying when users click on them. These strategies play a central role in increasing market visibility as well as attracting more visitors into the company's websites which in the long run may boost conversion rates. According to Kotler et al. (2021), digital disruptors in retail are more likely to use AI marketing than established retailers. Li and Zhang (2021) suggest that smaller online businesses can gain a competitive advantage by promoting themselves alongside larger brands using these strategies. AI marketing offers various advantages including increased activity and improved customer experience, reduced advertising waste, and more targeted campaigns (Stalidis et al., 2023). These advances in AI technology are

changing the way businesses interact with their customers, providing personalised experiences to increase loyalty and income. AI-powered insights can help marketers refine their strategies and achieve long-term success in a competitive market (Khrais 2020). AI automates routine tasks like data analysis and customer segmentation, allowing marketers to focus on strategic initiatives (Huang & Rust, 2021). AI's impact on marketing will grow, enabling businesses to engage with consumers in new ways (Kotler et al., 2021).

Another aspect of personalisation within e-commerce is the utilisation of recommendation systems to dynamically customise web layouts. Recommendation systems play a pivotal role in optimising product displays by arranging e-commerce pages based on client interests. Through personalised sort orders and dynamic adjustments to display columns, recommendation systems ensure that users are presented with relevant products tailored to their preferences and browsing history. (Zhang et al.2021; Chandra et al.2022, Fayyaz et al.2020). This 'flexible interface' approach shortens search times and increases client satisfaction (Ashfaq et al., 2020) with by focusing on trending products, providers can tailor search options to show popular items, allowing clients to make faster purchasing decisions and improving customer retention and satisfaction through post-purchase behavior analysis (Ramadan et al.2023; Alamdari et al.2020).That is why now, e-commerce sites are striving to improve the search experience, they know that clients expect a quick and relevant search result when they visit a website (Khrais, 2020; Wu et al., 2021; Gusenbauer and Haddaway, 2020).Understanding the role of AI-driven product recommendations is critical for providers in improving the product discovery process this approach reduces the difficulty of navigating into a list of products while increasing the likelihood of purchase, thereby improving the browse-to-purchase conversion rate (Thandekkattu and Kalaiarasi2022; Stone et al.2020; Khrais, 2020).

Artificial intelligence algorithms are expected to improve significantly in the near future (Rakha et al. 2020). Deep learning enables AI systems to generate trial data, self-discover, and predict with high accuracy (Singha et al.2021). Advancements in AI algorithms can significantly reduce execution time for recommendation systems (Zhang et al., 2021). As AI advances, recommendation systems are evolving from collaborative to hybrid models that combine AI and human preferences (Zhang et al., 2021). According to Kaushal and Yadav (2022), voice assistants are increasingly integrated into computer systems. According to Guo (2022), this

trend also applies to e-commerce platforms. Companies are increasingly integrating recommendation systems with voice assistants, including Alexa and Google Assistant (Klaus & Zaichkowsky, 2020). This trend relies on natural language processing (NLP) and context understanding to convert voice commands into useful data input (Khurana et al., 2023). E-Commerce platforms can use artificial intelligence and voice assistants to provide accurate and targeted product recommendations for a new generation of customers, leading to more effective and efficient marketing strategies (Kumar and Kumar2021). The customer experience has changed from physical goods and services to effortless personalised digital experiences as the world grows more digital (Hoyer et al. 2020). The user experience is changing due to the confluence of AI, machine learning, and big data analytics (Obschonka & Audretsch, 2020). Artificial intelligence enhances user experience by automating customer targeting and predictive analytics (Haleem et al.2022). The integration of AI-powered user experience enhancements into E-Commerce digital strategies is expected to elevate customer interaction with platforms (Balakrishnan & Dwivedi, 2021).

2.3 Privacy concerns

Privacy concerns refer to the fear regarding the potential misuse, unauthorized access, and improper handling of an individual's personal information (Manikonda et al., 2018). These concerns arise from the fear that personal data could be exposed, leading to adverse consequences such as identity theft, financial loss, and a loss of control over personal information (Carmody et al., 2021). Privacy concerns has emerged to be a crucial factor in AI systems, where personal information is frequently collected, processed, and stored by various online platforms.

Golda et al., (2024) adds that privacy concerns in AI are influenced by the extent and manner in which personal data is collected, how it is used, and the security measures in place to protect. It is important to note that, users of the online space are usually concerned about how much information is being gathered about them, including their browsing habits, purchase history, and personal preferences. Therefore, when there is a lack of clarity regarding how their data is going to be handled, the privacy concerns of users heighten.

The research study by Y. Liu et al., (2022) highlights that high levels of concern can lead users to limit the amount of personal information they share. When users feel that their privacy might be compromised, they become more cautious and selective about the information they

disclose. Consequently, users may choose to withhold certain details and avoid engaging with features that require extensive personal information, or even opt out of using platforms that exposes them to risk.

According to the research study by Shahriar et al., (2023), one of the ways that AI systems can use to mitigate the privacy concerns of users is compliance. Compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) and obtaining informed consent from users before collecting and using their data are essential in reducing the user's perception of risk.

2.4 Factors affecting Privacy concerns in AI Recommendation Systems

As the result of the widespread integration of AI, privacy concerns have emerged among the adopters of AI technologies. The privacy concerns have played a crucial role in affecting the consumer trust in the AI systems. The factors affecting consumer trust in AI recommendation systems can be better understood through the lens of the privacy calculus theory. The theory posits that individuals perform a cost-benefit analysis when deciding whether to disclose personal information (Wang et al., 2024). The theory analyzes how different people assess the perceived risks and perceived benefits of an action before making a decision. If the perceived risks are higher than the perceived benefits, individuals are less likely to disclose their personal information (Wang et al., 2024). Conversely, if the perceived benefits outweigh the risks, individuals are more likely to share their information. This theory helps explain the varying degrees of willingness to share personal data among consumers, especially in the context of digital environment. The following factors are critical in this context.

2.4.1 Perceived benefits

2.4.1.1 Personalisation

Personalization is one of the significant benefits of AI recommendation systems. Personalized services provide users with content, products, or services tailored to their preferences. This plays a crucial role in enhancing the user experience and satisfaction. Personalisation helps a company experience increased user engagement (Zanker et al., 2019). By providing relevant content aligned with specific needs and interests, users are more likely to interact with the brand, stay longer on the platform and make repeat visits. Additionally, Habil et al., (2023) added that personalization plays a central role in enhancing customer satisfaction and loyalty.

When a business meets the preferences of a consumer, there get satisfied with the offerings of the business. Companies can create a more personalized and engaging experience for customers. This customized approach not only increases satisfaction but also cultivates a stronger emotional connection with the brand, leading to increased loyalty and long-term relationships with customers (Naumov et al., 2019). The privacy calculus theory suggests that individuals weigh the perceived benefits of personalization against their privacy concerns when deciding whether to share personal information (Wang et al., 2024). When users perceive that the benefits of personalized services, such as tailored recommendations or enhanced user experiences, outweigh the potential risks to their privacy, they become more willing to disclose their personal data. When users perceive high value in the personalized services offered by AI systems, they may view the benefits as greater than the risks associated with data sharing.

Therefore, it is hypothesized that.

H1: Higher perceived benefits of personalization decrease the privacy concerns of users regarding AI recommendation systems.

2.4.1.2 Perceived anonymity of the Internet

It is important to note that using the Internet makes an individual feel a false sense of privacy and security. This can be partly credited to the perceived anonymity of the Internet. This means that people may feel safer when engaging with other individuals on the Internet than face to face interactions (Harborth & Pape, 2018). The perceived anonymity of the Internet can lead individuals to believe that their actions are not being monitored as closely as they might be in physical spaces (Wang et al., 2021). However, this perceived anonymity may be misleading as some agents may take advantage of this to exploit a user's privacy over internet platforms (Hite et al., 2014). Thus, while technology offers unprecedented convenience and connectivity, it also necessitates a heightened awareness of the risks to personal privacy and the importance of robust security measures to safeguard sensitive information in the digital realm.

The privacy calculus theory provides a framework for understanding the impact of perceived anonymity of the internet on a consumer’s privacy concerns. Internet users usually consider the perceived anonymity of the internet as a perceived benefit because it creates a sense of

security and freedom (Jiang et al., 2022). This allows them to engage in activities and share information without fear of immediate identification. This anonymity reduces the perceived risks associated with data sharing, as users believe that their personal information is less likely to be linked back to them directly (Chen, 2018). Consequently, the reduced perceived risk lowers privacy concerns, making users more willing to disclose personal information. This false sense of security, driven by perceived anonymity, illustrates a critical aspect of the privacy calculus where reduced perceived risk lowers privacy concerns, encouraging more open information sharing

Therefore, it is hypothesized that.

H2: Higher perceived anonymity of the Internet decreases the privacy concerns of users regarding AI recommendation systems.

2.4.2 Perceived risks

2.4.2.1 Data breaches

Another significant privacy factor that is related to AI recommendation systems is data breaches (Demirkan et al. 2020). If a hacker gains access to an AI recommendation system, a large amount of sensitive data could be compromised. Also, the algorithms that underpin these systems may begin to wrongly release personal information (Himeur et al., 2022). These concerns include an important component that is brought about by the possible risks of data breaches and illegal access.It is impossible to exaggerate the effects data breaches have on one's finances and reputation. According to a study conducted by John, Stachow, and Emigh (2011), 39% of consumers who were told of a data breach made 'significant' adjustments to their online activity, while 15% terminated or closed online accounts. This is notable evidence of a shift in consumer behavior in response to a lack of data security and privacy. Companies that lose sensitive client information may suffer long-term consequences including lost sales and reduced consumer trust in addition to immediate financial costs from damage control, legal bills, and possible fines (Gao et al., 2021). Additionally increasing the difficulties, the organisation faces in recuperating from a data breach is the possible loss of important employees or trouble bringing in top talent as a result of a damaged reputation. This situation emphasises how crucial it is to have strict security measures in place and keep data usage transparent in order to guard against unwanted access and maintain customer trust (Al Aina and Atan, 2020).

The privacy calculus theory posits that the perceived risk of data breaches plays a significant role in shaping privacy concerns. High perceived risks, such as those associated with data breaches, elevate privacy concerns and diminish trust in AI systems (Keith et al., 2013). The financial and reputational consequences of data breaches make users more cautious about sharing personal information. Data breaches can lead to significant changes in user behavior, as the perceived costs of information disclosure become too high.

Therefore, the following hypothesis is derived.

H3 Higher perceived risk of data breaches increases the privacy concerns of users regarding AI recommendation systems.

2.4.2.2 Consent risk

Another significant privacy factor in relation to AI recommendation systems is the consent factor. This is problematic since the data protection law has made it plain that the most important thing is to seek informed consent before using someone's data and to notify individuals about how their data will be used (Amaya et al., 2021). It is customary to withhold information about the collection of personal data from specific users and to refuse their request for consent. AI recommendation systems that collect personal information must adhere to local data protection legislation in the jurisdiction in which the system is hosted. Regarding the gathering, processing, storing, and use of personal data, these rules and regulations aim to protect persons' privacy (Ribeiro-Navarrete et al., 2021). In addition, the primary rule controlling the gathering and use of personal data is the user's consent, which the recommendation system would need to get. In cases where users have been informed about the collection and use of their personal information, consent may be obtained indirectly (Zhang et al., 2021). However, prior to doing so, precise rules governing the conditions under which an explicit consent might be transferred must be followed. These rules should specify the type of consent, whether it applies to the processing, transfer, and linking of various categories of personal data, as well as the extent, goal, and duration of the consent (Wang et al., 2022). Currently available modern facilities allows recommendation systems to adhere to the idea of privacy in practice. To decrease and manage informational privacy risks, this entails identifying and implementing the best privacy practices through organisation and policy, offering user-centric privacy solutions, and improving system design (Zhang et al., 2021).

The consent factor plays a crucial role in influencing the privacy calculus of an AI user (Singh, 2022). When users perceive a high consent risk, it means they are concerned about whether their consent has been obtained appropriately and whether they are truly aware of and agree with how their data is being used (Pickering, 2021). This includes concerns about the withholding of information, lack of transparency, and refusal to honor consent requests. Such practices can lead to a lack of trust in the AI system and increase users' privacy concerns.

Data protection legislation mandates that AI systems adhere to strict guidelines regarding the collection, processing, storing, and use of personal data to ensure privacy of the AI system users (Iserson, 2024). AI systems are required to obtain the user's explicit consent which must be given under specific precondition. When these conditions are met, and users feel confident that their consent is respected, their perceived risks decrease, and they are more likely to engage with the system. However, if the rules governing consent are not followed, users' privacy concerns escalate (Floridi et al., 2021). These concerns are amplified by fears of unauthorized data processing without the user's knowledge which exposes them to high consent risk.

H4: Higher perceived risk of consent issues increases the privacy concerns of users regarding AI recommendation systems.

2.5 Consumer trust

A myriad of research studies has dissected the concept and its aspects such as competence, ability, empathy, benevolence, integrity, and predictability (Gefen et al., 2003; Lee and Turban, 2001; McKnight et al., 2002; Urban et al., 1999). According to Luhmann (1979), trust is the basis of all social interactions. The different trust concerns have a fundamental impact on buyers' attitudes and behaviors toward sellers in the business world (Urban et al., 1999). One of the most common concepts in all the aspects of trust is that trust is inherent to uncertainty. (Hardin, 2002, p. 12). This suggests that the essence of trust often manifests in situations characterised by the absence of complete predictability of outcomes. Additionally, another concept that is prevalent in all the concepts of trust is that the need of trust arises in a risky situation. This implies that the need for trust arises in contexts where the outcomes are potentially detrimental (Mayer et al., 1995, p. 711). Additionally, a defining concept of trust that is highlighted by numerous research studies is that "trust exists in an uncertain and risky environment" (Bhattacharya et al., 1998, p. 461). It is believed that trust is essential to reducing

risk and uncertainty in online buyer-seller relationships because of the complicated and unpredictable nature of online transactions (e.g., Ha and Stoel, 2008; McKnight and Chervany, 2002; Mayer et al., 1995).

The research study by Manzini et al., (2024) highlighted two factors that enable users trust AI assistants, which include competence and alignment. According to the research by Manzini et al. (2024), competence is a foundational aspect of justified trust. Trust in system competence pertains to users' belief in the ability of the AI system to perform its intended functions effectivel. Competence directly affects the user's willingness to rely on the recommendations provided by an AI system (Ryan, 2020). When users perceive the AI system as competent, they believe that it can analyze their preferences accurately to deliver personalized recommendations. Competence trust is built through consistent and positive interactions with the system (Ryan, 2020). For instance, if an AI recommendation system consistently suggests products that match a user's preferences, the user is more likely to develop trust in the system's competence.

On the other hand, alignment pertains to the belief that the AI recommendation system operates in a way that aligns with the user's values and interests (Manzini et al., 2024). Alignment focuses on the ethical use of personal data, the transparency of data handling practices, and the adherence to privacy and security standards. Users develop alignment trust when they feel assured that the system will protect their personal information and use it responsibly. Manzini et al. (2024) emphasize that alignment between the interests, values, or incentives of AI assistants, developers, and users is critical for fostering trust. Misalignment can lead to situations where users' expectations are betrayed, causing significant harm.

2.6 Relationship between privacy concerns and consumer trust

Research has shown that privacy concerns are a critical determinant of consumer trust in online environments. For instance, studies by Bansal et al., (2015) highlight that privacy assurances are essential for building consumer trust in e-commerce platforms. By providing clear information about how user data is collected, stored, and utilized, e-commerce platforms can help users feel more confident about sharing their personal information (Ozturk et al., 2017). Transparent privacy policies, secure data handling practices, and effective communication about privacy safeguards all contribute to fostering trust among consumers,

ultimately encouraging them to engage more with the brand. This trust, in turn, influences users' willingness to engage with these platforms and share their personal information.

Martin and Murphy (2017) also mention that the consumers' trust levels and subsequent involvement with online shops are significantly shaped by privacy concerns. People are more likely to show less trust in online shops when they are more concerned about the security and privacy of their personal information (Martin and Murphy (2017). This mistrust may operate as a discouragement, affecting users' willingness to engage with online services and make purchases. Hann and Hui (2007) add that perceptions of privacy intrusions have indeed the power to affect consumer confidence and discourage them from transacting when they are asked for personal information. Hence, the majority of customers emphasise the value of privacy in fostering customer trust and are sensitive to concerns about the privacy of online information.

Separating perceived from real privacy dangers is essential to understanding the interactions between privacy concerns and consumer trust**.** When a consumer browses on an e-commerce platform, user data such as search history, clicked links, and time spent on pages is collected and analysed to create personalised recommendations. While personalised recommendations can enhance user experience, users may be concerned about the privacy implications of this data tracking. They may worry that their information is being used for targeted advertising or other purposes without their explicit consent. If a data breach occurs, the information may be released to third parties without consent, making it a potential privacy risk (Yang et al., 2020).On the other hand, "perceived privacy risk" refers to circumstances in which a person's information is gathered and utilised for a particular purpose, but the person is worried—based on their perception rather than actuality—that this information may be misused for other purposes (Balapour et al. 2020). This distinction is crucial because perceived privacy risks center on building consumer confidence and trust in e-commerce, but actual privacy concerns primarily concern data protection (Zhang et al. 2020).

Bhattacharya et al. (2023) emphasise the emotional response to perceived privacy threats as an important factor in understanding the relationship between consumer trust and privacy concerns. According to a study, customers who feel as though their privacy has been violated report feeling scared, anxious, and concerned, all of which lower their trust levels (Khatoon and Rehman2021). A strong correlation was found after more than 2,000 customer comments

were analysed in response to a US Federal Trade Commission request regarding internet privacy. According to Chen et al. (2022) there is a 16% decrease in the likelihood that consumers will maintain trust for every increase in negative sentiment. However, trust tendency, or the desire to trust, is crucial; people who have a strong propensity to trust appear to be more resilient to the negative impacts of privacy concerns on trust (Tian et al., 2022). Although privacy issues have an impact on consumer trust, their influence is significantly lessened in those who are already inclined to trust (He et al., 2021). In order to improve consumer engagement and confidence in digital transactions, e-commerce platforms must adopt tailored strategies that both foster trust and effectively address privacy concerns. This is because the interaction between an individual's innate trust propensity and external privacy threats poses a nuanced challenge (Aslam et al. 2020).

According to Chen et al. (2021), building consumer trust requires consistent advantageous user experiences and human connections over time. It is based on the notion that people who divulge personal information to an organisation, like their address and bank account details, would respect that information and not abuse the trust that has been placed in it (Giao et al.2020). When a privacy violation occurs, the underlying trust is frequently affected. According to Muhammad et al. (2022), firms may underestimate the impact of a violation on consumer trust. Munn (2023) identifies various forms of damage control, such as monetary losses from reduced sales and retention of clients, loss of brand value and reputation, and missed opportunities to invest in business development and success. According to Zhang et al. (2020), regulators and advisory bodies are emphasising the importance of consumer trust in privacy and consumer protection. The European Data Protection Supervisor recommends that privacy laws prioritise fostering user trust in digital services (Monzer et al., 2020). As more firms move online, it's crucial to maintain user trust (Melović et al., 2020).

Privacy concerns can negatively impact consumer trust in corporate relationships (Cheah et al.2022). This relationship appears to be most significantly impacted by the consumer's decreased desire to provide personal information. Digital marketing and customer feedback, such as star ratings and reviews, enable businesses to build personalised relationships with customers and better meet their unique needs (Lin et al., 2021). Businesses that lack the necessary information to accurately communicate and suggest products based on individual needs limit their ability to create personal partnerships and provide services that meet modern

consumer needs (Cheng & Jiang, 2022). When a business is unable to do this, the consumer is significantly less likely to be able to engage in the type of rich, personal, and mutually beneficial connection that is achievable when the firm understands how to best serve the consumer. Customers' contentment, sense of belonging, and access to high-quality services and products would all be impacted (Cheng & Jiang, 2020). To fully understand the impact of privacy concerns on the consumer-business relationship (Gao et al., 2021), it's important to be aware of the negative consequences of a decrease in willingness from both parties.

Research studies have also highlighted the impact of privacy concerns on trust in the systems competence. Trust in system competence refers to the belief that the AI system can effectively perform its intended functions (Gieselmann & Sassenberg, 2023). When privacy concerns are high, users may doubt the system's ability to protect their personal information. (Long & Magerko, 2020) add that users may associate poor data protection with a lack of technical proficiency. For example, if users fear that their data could be easily breached or misused, they might question whether the system is competent enough to provide accurate and reliable recommendations. High privacy concerns can lead users to perceive the system as unreliable.

Therefore, it is hypothesized that.

H5: Higher privacy concerns decrease users' consumer trust in the competence of an AI system.

Multiple research studies have also investigated on the impact of privacy concerns on the trust in the system alignment. High privacy concerns may make a user feel that system's data practices are not aligned with their expectations of privacy and ethical behavior (Gabriel & Ghazavi, 2021). When users are concerned about how their data is handled, they may perceive a misalignment between their values and the system's operations. For instance, if users believe that their data is being used for purposes beyond their consent, they may view the system as operating unethically. (Aguirre et al., 2020) adds that alignment trust is crucial for long-term user engagement. When a user feels a sense of consistency and reliability in the system’s operations, they are likely to repetitively interact with the system which in the long run contributes to user loyalty.

Therefore, the research study hypothesizes that.

H6: Higher privacy concerns decrease users' trust in the system's alignment.

2.7 Conceptual framework

Conceptual framework is a visual presentation of the relationships between the independent variables, mediating variables and the dependent variables (Jabareen, 2009). The figure below defines the Conceptual framework for the research process.

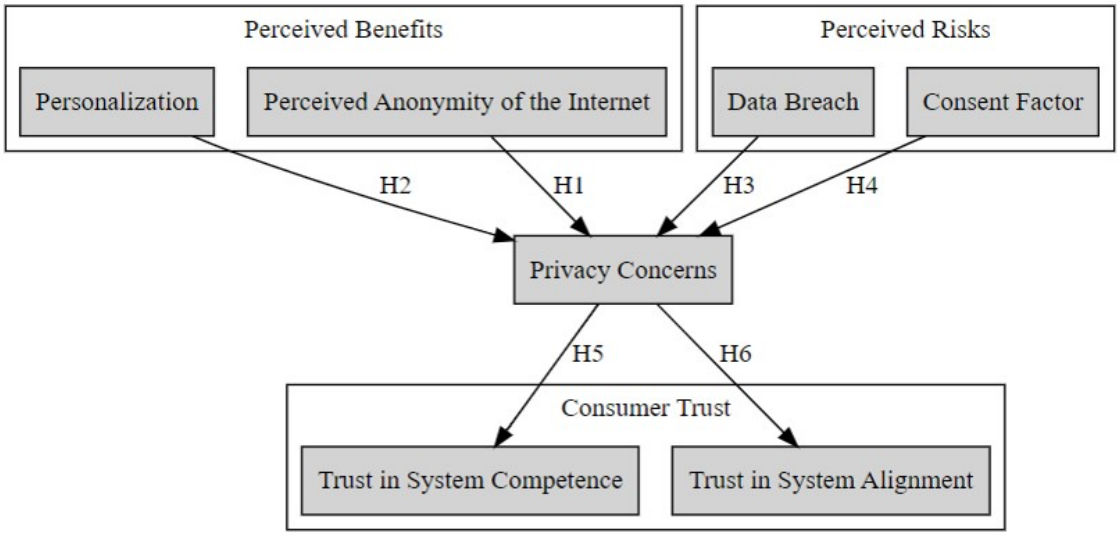

Figure 1 Showing the Conceptual Framework

3 METHODOLOGY

3.1 Introduction

The main objective of this research study is to evaluate the impact of AI-driven personalisation tools on privacy concerns of E-commerce customers. This chapter presents the research methods that the researcher is going to utilise to achieve the research objectives. The preliminary part of this chapter will describe the research approach that the researcher is going to use for this research study. Thereafter, the research design will follow, whereby the researcher will indicate the data collection and data analysis methods that the researcher will use to achieve the research objectives. Moreover, the concluding part of this chapter will describe the ethical principles that the researcher has adhered to in the research process.

3.2 Research Approach

Research approach refers to the overreaching research strategy that guides the direction and execution of the research process. Saunders et al., (2015) defines two forms of research approach, namely the deductive research approach and the inductive research approach. The deductive research approach entails conducting a preliminary literature review and developing a hypothesis based on existing theories, thereafter, designing a research methodology that tests the hypothesis and draws meaningful conclusions from the analysis (L. Liu, 2016). It is important to note that the deductive research approach is associated with quantitative research methods, where the data collected for the analysis is numerical, and statistical tools are used for the analysis (L. Liu, 2016). On the other hand, the inductive research approach entails making preliminary specific observations and developing a general theory based on those observations (Young et al., 2020). The process of an inductive research approach entails observing patterns, making generalisations and forming hypotheses based on those patterns. It is important to note that the inductive research approach is mostly associated with qualitative research methods where the data is descriptive and is gathered through methods such as interview discussions and observations.

This research study adopts the deductive research study because it starts from a general theory to specific observations. For this research study, the researcher develops a hypothesis based on the privacy calculus theory. Thereafter, the researcher develops questionnaires,

collects data, analyses it and tests the hypothesis to derive meaningful conclusions from it, which is consistent with the deductive research approach.

3.3 Population and Sampling design

3.3.1 Population

Cooper et al., (2006) defined population as the collection of items under consideration under a research study. Alternatively, the research study by Creswell & Creswell, (2017) defined population as composite number of study units in a research area. The population that was used for this research study are Amazon Reviewers in Belgium.

3.3.2 Sampling design

A sampling design refers to the technique that a researcher uses in the process of selecting a sample from a given population (Burger & Silima, 2006). A sampling design helps researchers select a smaller representation of the population, mitigating the need to handle the entire population while maintaining the characteristics of the population. Taherdoost, (2016) defines two categories of sampling design, namely, the probabilistic sampling design and the non-probabilistic sampling design. A probabilistic sampling design uses random selection, giving every member of the population an equal chance of being selected. A non-probabilistic sampling design uses bias to select the sample based on the researcher's preferences.

This research employs a non-probabilistic sampling design known as convenience sampling. This is a sampling design whereby participants are selected based on their availability. Convenience sampling was selected because of its efficiency, as the researcher could easily gather data from participants who met their preferred criteria. In addition, convenience sampling is a cost-effective method of recruiting participants.

3.4 Data Collection

There exist two primary methods of data collection, namely primary methods and secondary methods (Saunders et al., 2015). Primary methods of data collection entail collecting data firsthand for a specific purpose. On the other hand, secondary methods entail using existing data that has already been collected by other sources for other purposes.

This research study employs both primary and secondary methods of data collection. The secondary method of data collection is used in the literature review section, whereby the researcher gathered and analysed existing research articles and scholarly sources that are

relevant to this research study. The secondary data collection through the literature review phase provided the context and framework for the primary data collection. The primary data collection was conducted using the survey instrument. A survey was administered to selected Amazon reviewers using the Lime survey tool.

3.4.1 The Survey Structure

A survey was administered to selected Amazon reviewers using the Lime Online survey tool. It offers a robust and user-friendly platform that simplifies the survey creation process. Its extensive customization options enable us to tailor the survey to our specific research needs. In addition, the platform enables the user to easily distribute the survey via email or direct links, reaching a diverse and relevant sample efficiently.

Before the researcher shares the survey to the targeted respondents, the researcher carried out a pilot test with 5 participants. testing the survey with a small group enabled the researcher to check if the questions are clear and understandable by the targeted respondents. In case there is some sense of ambiguity, the researcher may rephrase the questions to avoid ambiguity and make sure the respondents appreciate the set questions. A trial test is also conducted to check if the survey is it is too long or might lead to respondent fatigue and henceforth incomplete responses. If the trial respondents do not complete, it proves that the survey tool will not be effective. The pilot test also checks for technical aspects, such as usability of the platform on various devices by the respondents.

The preliminary section of the survey consists of questions to check on the demographic information of the respondents such as gender, age, level of education. Demographic factors help the researcher understand the composition of the respondents and providing context for interpreting the survey results (Klimczuk, 2021). In addition, demographic data helps in identifying patterns and trends within specific groups, which can be crucial for analysing how different segments of the population perceive and respond to the factors being investigated.

3.4.2 Scales and Measurements

The table below provides an overview of the seven research constructs that the researcher measured using statements. The researcher was expected to state the level to which they agree with the statements.

Construct	Scale	Item	Statement

IV **Personalisation** (Zanker et al., 2019) (Habil et al., 2023) (Naumov et al., 2019) (Wang et al., 2024)	5-Point Likert Scale (From 1 Strongly disagree to 5 Strongly agree)	PS1	I often receive personalised product recommendations when shopping online.
		PS2	Online advertisements seem tailored to my interests and preferences.
		PS3	E-commerce platforms suggest products based on my past purchases or browsing history.
		PS4	I frequently encounter personalised content or recommendations while using e-commerce websites
IV **(Perceived anonymity of the Internet)** (Harborth & Pape, 2018) (Hite et al., 2014) (Jiang et al., 2022)	5-Point Likert Scale (From 1 Strongly disagree to 5 Strongly agree	PA1	I feel safer making online purchases because I don't have to interact with sellers face-to-face.
		PA2	I believe my personal information is more secure when I'm online compared to offline.
		PA3	I trust that my identity remains anonymous when I engage in online activities.
		PA4	I perceive the Internet as a place where I can maintain my privacy better than in physical stores.
IV **(Data Breach)** (Demirkan et al., 2020) (Gao et al., 2021) (Himeur et al., 2022)	5-Point Likert Scale (From 1 Strongly disagree to 5 Strongly agree	DB1	I am concerned that my personal data might be compromised in a data breach.
		DB2	I worry about the security measures in place to protect my personal information on e-commerce websites.
		DB3	I fear that my financial information could be stolen during online transactions.
		DB4	I am anxious about the possibility of hackers accessing my personal data on e-commerce platforms.
IV **Consent risk** (Singh, 2022) (Pickering, 2021) (Floridi et al., 2021)	5-Point Likert Scale (From 1 Strongly disagree to 5 Strongly agree	CR1	I am informed about how my personal data will be used before I give consent.
		CR2	I am confident that my consent is obtained explicitly before my data is collected.
		CR3	I trust that the AI recommendation system respects my consent regarding data usage.
		CR4	I believe that I am given enough information to make an informed decision about my data consent.
MV **Privacy concerns** (Bansal et al., 2015) (Ozturk et al., 2017) (Carmody et al., 2021) (Golda et al., 2024)	5-Point Likert Scale (From 1 Strongly disagree to 5 Strongly agree	PC1	I am concerned about the amount of personal information that e-commerce platforms collect.
		PC2	I worry that my personal data might be shared without my consent.
		PC3	I feel uneasy about the ways my data is used by e-commerce websites.
		PC4	I am anxious about the potential misuse of my personal information online.
DV **Trust in AI Competence**	5-Point Likert Scale (From 1 Strongly disagree	TC1	I believe that the AI recommendation system provides accurate recommendations.

(Gieselmann & Sassenberg, 2023) (Long & Magerko, 2020)	to 5 Strongly agree	TC2	The AI recommendation system meets my needs for product recommendations.
		TC3	The AI recommendation system consistently delivers high-quality recommendations.
		TC4	I The AI recommendation system uses advanced technology to provide useful recommendations.
DV **Trust in AI Alignment** (Gabriel & Ghazavi, 2021) (Aguirre et al., 2020)	5-Point Likert Scale (From 1 Strongly disagree to 5 Strongly agree	TA1	The AI recommendation system is honest about how it uses my personal information.
		TA2	The AI recommendation system provides fair and unbiased recommendations.
		TA3	I trust the AI recommendation system to protect my personal information.
		TA4	The AI recommendation system is responsible in handling my personal data.

As observed in the above table, each research construct consisted of statements that the researcher needed a response to. The researcher expected the participants to respond on a measurement scale of 'strongly disagree,' 'disagree,' 'neutral,' 'agree,' and 'strongly agree.' These responses were made on a numerical response scale ranging from 1 to 5, where 1 represented 'strongly disagree,' 2 represented 'disagree,' 3 represented 'neutral,' 4 represented 'agree,' and 5 represented 'strongly agree.' This standardised scale allowed participants to provide consistent and quantifiable responses, facilitating analysis and interpretation of the survey data.

The researcher conducted a Reliability of the survey to check on the internal consistency of the survey instrument that was developed. Internal consistency refers to the extent to which all the items in a survey measure the same underlying construct (Vaske et al., 2017). High internal consistency suggests that the survey items are coherently measuring the same concept, which in turn supports the validity of the findings. In addition, reliability of the research instrument enables the researcher to ensure that the survey instrument produces consistent results over time contributes to the overall quality of the survey data (Vaske et al., 2017). Reliability test was conducted by analysing the Cronbach alpha coefficient of the measurement scales in the SPSS statistical software.

3.5 Data Analysis

Saunders et al., (2015) defines data analysis as the process of examining data with the aim of obtaining useful information and insightful conclusions from it. Data analysis can be

categorised into qualitative data analysis and quantitative data analysis. Qualitative data analysis is the process of examining non-numerical data such as text, audio, and images to observe patterns and obtain insights. On the other hand, quantitative research design entails the application of statistical tools and mathematical methods to evaluate numerical data so as to establish relationships and trends within the data.

This research study adopted the quantitative data analysis method. After the data was collected using the Lime survey tool, the data was exported to the Excel program, where the researcher sorted and cleaned it. Thereafter, the data was exported to the SPSS statistical software for the extensive data analysis process. The data analysis process was categorised into two phases, which were the descriptive statistics phase and the inferential statistics phase.

3.5.1 Descriptive statistics phase

The Descriptive statistics phase entails describing the key characteristics of the data. In this phase, the researcher started by conducting a demographic analysis. The demographic entails assessing the demographic variables of the participants, such as age, gender and education level. Thereafter, the researcher evaluated measures of central tendency, measures of dispersion and frequency distributions.

3.5.2 Inferential statistics phase

The inferential statistics phase goes beyond data description to making generalisations about the population based on the sample data collected. The inferential statistics phase will entail correlation analysis, regression analysis, ANOVA tests and hypothesis testing. The researcher used the results of these tests to draw conclusions, which gave answers to the research questions. In this way, the objectives of the research study were achieved.

3.6 Ethical Considerations

It is imperative for a researcher to define ethical considerations so as to ensure the protection of the rights of the participants and integrity throughout the research process (Nafsi, 2023). A research process that adheres to ethical principles of research demonstrates the researcher's commitment to upholding professional standards and social responsibility (Khan, 2015). To achieve this, the researcher sent a consent letter to all the participants informing them that their data was going to be used for an academic thesis. The consent letter assured the participants of the confidentiality of their identity and the privacy of their personal

information. The consent form also provided the option of voluntary withdrawal in case the participant chose to cancel their submissions. Thereafter, the consent letter was sent to the University Research Ethics Committee before administering the survey to the participants.

4 RESULTS

4.1 Introduction

This research study sought to investigate the impact of AI-driven personalisation tools on privacy concerns and consumer trust in e-commerce. To achieve this, the researcher conducted a preliminary literature review, which helped to determine the research variables that were used to develop a questionnaire. The questionnaires were administered to select Amazon reviewers. The questionnaires were administered through the Lime survey tool and analysed using the SPSS statistical software. This chapter presents the findings of the data analysis that was conducted using SPSS software. The preliminary sections of this chapter first describe the respondents, conduct a reliability and validity test, and present a descriptive analysis of the data. Thereafter, the researcher will conduct a regression analysis, which will enable the researcher to test the hypotheses and draw relevant conclusions. Thereafter, the researcher will discuss the findings in a relevant way.

4.2 Respondents

The questionnaire was administered to respondents over the course of one week. The respondents were obtained from the product review section at Amazon as well as online communities such as Facebook groups that Amazon users connect with. The main channels through which the survey was distributed were through social media platforms such as Whatsapp, Facebook, and Instagram. The target number of answers was reached in record time, after which the survey was closed to avoid any additions to the database. The survey gathered a total of 453 responses. The data was exported to an Excel document. The data underwent a cleaning process to remove incomplete responses and entries with missing values. Specifically, 140 entries were removed, and the final data had 313 responses. The data cleaning and validation process was to ensure that only complete and accurate responses were included in the analysis.

The survey included two socio-demographic questions; one was meant to investigate the gender distribution, and the other investigated the age distribution. For the gender distribution data, the majority of the respondents, representing 53% of the data, were male, while 47% of the data were female respondents. The results show a relatively balanced distribution between male and female participants, which implies that the findings from the study are less likely to be biased toward one gender. Table 1 and Figure 1 below give a detailed

description of the gender distribution data. For the age distribution data, the majority of the respondents, representing 39% of the data, were between 18- and 24-years age bracket. 31% of the participants were between the ages of 21 and 34, 16% of the respondents were between 25 and 44 years, 7% of the respondents were in the range of 35 and 54 years, 4% of the respondents were under 18 years and 3% of the respondents were above 55 years. Most of the respondents fall in the 18 to 24 and the 25 to 34 age brackets. This implies a youthful skew in the data. This high response by participants in these youthful age brackets can be attributed to their heavy presence on digital platforms compared to the older generation. On the other hand, there is less representation of the older age brackets, which might be due to their less familiarity with digital technologies. More details of the age distribution data are provided in the table below, and its visual representation is found in a pie chart in Figure 1 below.

		Frequency	**Percentage distribution**
Gender	Male	166	53%
	Female	147	47%
Age bracket	Under 18 years	14	3%
	Between 18 and 24 years	121	39%
	Between 25 and 34 years	98	31%
	Between 35 and 44 years	49	16%
	Between 25 and 54 years	21	7%
	Above 55 years	10	4%

Table 1 Showing the Age and gender distribution data.

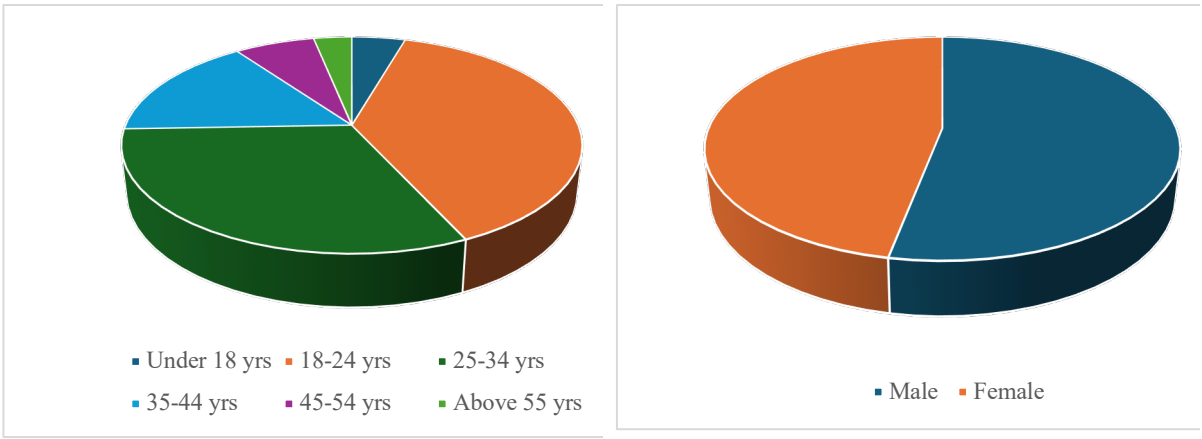

Figure 2 shows the visualisation of the age and gender distribution data.

4.3 Reliability and Validity analysis

4.3.1 Cronbach alpha tests

The researcher used the Cronbach alpha test to measure the reliability of the constructs used in the questionnaire. The Cronbach test measures the internal consistency of a set of items that are intended to measure a single latent construct. This helps to give the researcher insight into the reliability of the scales that they used in the survey. A Cronbach's alpha value of greater than 0.7 indicates high internal consistency, which means that the items within a scale are highly correlated (Vaske et al., 2017). The Cronbach alpha test was done using the SPSS software. The results are summarised in the table below.

Scale	**Cronbach Alpha**	**Number of items**
PS Scale	0.792	4
PA Scale	0.772	4
DB Scale	0.811	4
CR Scale	0.687	4
PC Scale	0.794	4
TC Scale	0.799	4
TA Scale	0.707	4

Table 2 shows results of the Cronbach alpha analysis

The PS scale showed strong internal consistency with an alpha of 0.792. Similarly, the PA scale recorded an alpha of 0.772, supporting its reliability in measuring the perceived anonymity of the Internet. The DB scale demonstrated very good reliability with an alpha of 0.811. However, not all scales reached the desirable consistency level. The CR scale recorded a lower alpha of 0.687, falling just below the accepted benchmark of 0.7. The CR Scale, though acceptable, shows that the scale may be less consistent in measuring the construct. The PC, TC, and TA scales have high alphas of 0.784,0.799 and 0.707. Generally, these results affirm that the scales that were used in the questionnaire are reliable for measuring the respective constructs. The high levels of internal consistency support the use of these scales for further analysis in the study.

4.3.2 Factor analysis.

This research study conducts factor analysis separately for the independent variables and the dependent variables.

4.3.2.1 Independent variables

The independent variables are basically the perceived benefits and the perceived risks of using AI-driven personalisation tools. The perceived benefits include Personalisation (PS Scale) and Perceived anonymity of the Internet (PA Scale). The Perceived risks consisted of Data Breach (DB Scale) and Consent risk (CR Scale). For these scales, the researcher conducted an EFA using the Principal Component Analysis and the Varimax rotation. The minimum factor loading was set at 0.5.

After the test was run, some of the extraction values in the communalities table were below 0.5. This included values of PA1, CR1 and CR4, as seen in Appendix 7.1. Therefore, these elements were removed. After they were removed, all the extraction values were more than 0.5, indicating a sufficient amount of variance in each variable is explained by the factors.

As shown in Appendix 7.2, the KMO test was also used to check if the data was appropriate for a factor analysis. Since the KMO was 0.797, which is greater than 0.05, this indicated that the data is appropriate for factor analysis. In addition, the weight of the correlation matrix was checked using Bartlett's Test of Sphericity. Since the results were significant, with a P value of less than 0.01, the variables correlate with each other, which means that the data is appropriate for factor analysis.

Appendix 7.3, titled 'Total Variance Explained', helps to identify the selected factors. Components with eigenvalues of less than 1 are excluded because they explain less variance. The final Component matrix with four components is displayed below. According to the diagram below, the variables were grouped according to the components or factors they loaded onto. After Varimax rotation, all the variables had a high loading on a specific factor, indicating a strong relationship with the component. Therefore, the findings of this analysis indicate a good factor solution.

Rotated Component Matrix				
Component				
Variables	**1**	**2**	**3**	**4**
PS1	0.802			
PS2	0.752			
PS3	0.692			

PS4	0.771			
PA2			0.816	
PA3			0.816	
PA4			0.833	
DB1		0.667		
DB2		0.752		
DB3		0.845		
DB4		0.798		
CR2				0.763
CR3				0.859
Extraction Method: Principal Component Matrix Rotation: Varimax with Kaiser normalisation				

Table 3 shows the component matrix for independent variables

4.3.2.2 Dependent variables

The dependent variables were used to measure consumer trust. Trust was measured in two dimensions: Trust in AI Competence (TC Scale) and Trust in AI Alignment (TA Scale).For these scales, the researcher conducted an EFA using the Principal Component Analysis and the Varimax rotation. The minimum factor loading was set at 0.5.

According to the results displayed in Appendix 7.5, the extraction value of the TA4 scale was below 0.5; hence it was removed. After the scale was removed, all the extraction values were more than 0.5., indicating that a sufficient amount of variance in each variable is explained by the factors. As seen in Appendix 7.6, the KMO test was also used to check if the data was appropriate for a factor analysis. Since the KMO was 0.749, which is greater than 0.05, this indicated that the data is appropriate for factor analysis. In addition, the weight of the correlation matrix was checked using Bartlett's Test of Sphericity. Since the results were significant, with a P value of less than 0.01, the variables correlate with each other, which means that the data is appropriate for factor analysis.

Components with eigen values of less than 1 are excluded because they explain less variance as shown in Appendix 7.7 . The final Component matrix with four components is displayed below. According to the table below, the variables were grouped according to the components or factors they load onto. After Varimax rotation, all the variables had a high loading on a specific factor, indicating a strong relationship with the component. Therefore, the findings of this analysis indicate a good factor solution.

Rotated Component Matrix		
Component		
Variables	**1**	**2**
TC1	0.794	
TC2	0.801	

TC3	0.778	
TC4	0.752	
TA2		0.763
TA3		0.654
TA4		0.825
Extraction Method: Principal Component Matrix Rotation: Varimax with Kaiser normalisation		

Table 4 shows rotated component matrix for dependent variables

4.4 Descriptive analysis

The table below shows a summary of the key descriptive statistics for each of the scales that were derived from the data analysis in the SPSS statistical software. The descriptive statistics that are analysed include the mean, standard deviation, skewness, kurtosis, and the normality test: Kolmogorov Smirnov test. Kolmogorov Smirnov test was used because it is used to test normality for data that is greater than 100, as opposed to Shapiro Wilk, which is used to check normality for data sets less than 100 (Das & Imon, 2016).

Statistic	**PS**	**PA**	**DB**	**CR**	**PC**	**TC**	**TA**
Mean	3.9593	2.3363	3.9249	3.0799	3.9768	3.7308	3.0751
Standard deviation	0.8183	0.85798	0.84871	0.73462	0.7944	0.82214	0.74863
Skewness	-1.661	0.99300	-1.4000	0.1610	-1.532	-1.068	0.1380
Kurtosis	2.452	0.645	1.644	0.3790	2.564	1.025	0.348
K-Smirnov Statistic	0.239	0.144	0.219	0.163	0.215	0.168	0.131
df	313	313	313	313	313	313	313
Sig	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Table 5 shows the results of the descriptive analysis.

The mean value for (PS) scale was 3.9593, with a moderate standard deviation of 0.8183. The high mean value (towards Agree value 4) indicates a generally positive perception of the personalisation capabilities of AI-driven personalisation tools. However, the negative skewness of -1.661 suggests that while a majority of respondents rated Personalization highly, there are some who rated it significantly lower. On the other hand, the Kolmogorov-Smirnov test was used to check for the normality of the data. As seen in the table above, the p-value is less than 0.05, which means that the result is statistically significant. Therefore, this implies that the data in the PS scale is not normally distributed. Results of transformed logs of the PS scale, as shown in Appendix 7.9, confirmed that the data does not follow a normal distribution since the p values were still less than 0.05.

On the other hand, the mean value for the PA scale was 2.3363, with a relatively higher standard deviation of 0.857. The relatively low mean (disagree value 2) indicated that respondents do not perceive a high level of anonymity on the Internet when interacting with AI-driven systems. The positive skewness of 0.99300 indicates that while the majority of

respondents rated anonymity lower, some rated it higher. The K-Smirnov test shows a p-value less than 0.05, indicating statistical significance and suggesting that the data in the PA scale is not normally distributed. The Kolmogorov-Smirnov test was also run on the transformed logs of the PA scale, as shown in Appendix 7.9. This confirmed that the data did not follow a normal distribution since the p-values were still less than 0.05.

For the DB scale, the mean was 3.9249. The high mean (towards agree value 4) reflects considerable concern among respondents about data breaches associated with AI-driven personalisation tools. The negative skewness of -1.4000 suggests that while many respondents have high concerns, some have rated it significantly lower. The K-Smirnov test results shown in Appendix 7.9 indicate a p-value less than 0.05, meaning that the data in the DB scale is not normally distributed. The K-Smirnov test was also run on the transformed logs, but still, the data did not follow a normal distribution since the p values were still less than 0.05.

Additionally, the CR scale had a mean of 3.0799. This moderate mean (neutral value 3) suggests a varied perception of consent risk among respondents. The skewness is 0.1610, indicating a nearly symmetrical distribution, with opinions spread across the scale. The K-Smirnov test shows a p-value less than 0.05, which implies that the data in the CR scale is not normally distributed. The K-Smirnov test was also run on the transformed logs of the PCR scale, as shown in Appendix 7.9. This confirmed that the data did not follow a normal distribution since the p-values were still less than 0.05.

The mean value for the PC scale was 3.9768. The high mean (towards agree value 4) indicates that respondents generally have significant privacy concerns when using AI-driven personalisation tools. The negative skewness of -1.532 suggests that while most respondents have high privacy concerns, a few rated it lower. The K-Smirnov test results in a p-value less than 0.05, showing that the data in the PC scale is not normally distributed. The K-Smirnov test was also run on the transformed logs of the PC scale in Appendix 7.9. The p-values of less than 0.05 showed statistical significance, which confirmed that the data does not follow a normal distribution

Moreover, the mean value for the TC scale was 3.7308. This relatively high mean (towards agree value 4) suggests that respondents generally trust the competence of AI systems. The negative skewness of -1.068 indicates that while many respondents rated their trust in AI

competence highly, some rated it lower. The K-Smirnov test shows a p-value less than 0.05, suggesting that the data in the TC scale is not normally distributed. The K-Smirnov test was also run on the transformed logs of the TC scale, as shown in Appendix 7.9. This confirmed that the data did not follow a normal distribution since the p-values were still less than 0.05.

Finally, the TA scale had a mean of 3.0751. This moderate mean (neutral value 3) indicates a varied level of trust in AI alignment among respondents. The skewness of 0.1380 suggests a relatively symmetrical distribution. The K-Smirnov test results in a p-value less than 0.05, indicating that the data in the TA scale is not normally distributed. Further descriptive statistics of the transformed logs of the PTA scale, as shown in the Appendix, 7.9confirmed that the data does not follow a normal distribution since the p values of the Kolmogorov Smirnov were still less than 0.05.

4.5 Regression analysis

Since the data does not follow a normal distribution, this implies that the researcher is required to use non-parametric methods of data analysis. In this case, the researcher used ordinary regression analysis to test the hypotheses. For this case, the researcher ran three regressions.

4.5.1 Regression 1: Predicting Privacy concerns.

The first regression was used to test H1, H2, H3, and H4. This analyses the relationship between the four independent variables (perceived anonymity of the Internet, perceived benefits of personalization, perceived risk of data breaches, perceived risk of consent issues) and privacy concerns. Ordinal regression was used, and the following results were established.

4.5.1.1 Model fitting checks.

The results of the model fitting checks are presented in the table below.

Model	-2Log likelihood	Chi-Square	Df	Sig
Intercept only	1370.988			
Final	1208.175	162.813	4	0.000
Link function: Logit				

Table 6 shows model fitting checks for Regression 1

The model-fitting information provided in the table is crucial for assessing whether the ordinal regression model fits the data well. The significant p-value of 0.000 confirms that the model is

a good fit, meaning that the relationships between the predictors and the outcome variable (PC) are meaningful and statistically significant.

4.5.1.2 Parameter estimates

The results for the parameter estimates are presented in the table below.

Variable	Parameter estimate	Std. error	Df	Sig.
PS	-0.499	0.145	1	0.001
PA	-0.206	1.135	1	0.120
DB	1.742	1.164	1	0.000
CR	0.033	1.52	1	0.830

Table 7 shows regression coefficients for regression 1

The estimate for PS is -0.499, which is negative and statistically significant, p = 0.001. This suggests that as perceptions of personalisation increase, the levels of privacy concerns decrease. The parameter estimate for PA is -0.206. Although the estimate is negative, indicating a potential negative relationship, the lack of significance means there is no sufficient evidence to support the hypothesis. The estimate for DB is 1.742, which is positive and highly statistically significant, with a p-value of less than 0.05. This large and significant estimate suggests that concerns about data breaches are strongly associated with higher levels of privacy concerns. The estimate for CR is 0.033, which is not statistically significant (p = 0.830), because it is greater than 0.05. This suggests that concerns about consent do not significantly influence privacy concerns in this model.

Therefore, the following table presents the results of the hypothesis results related to the above results.

Code	Hypothesis	Sig	Result
H1	Higher perceived benefits of personalisation decrease the privacy concerns of users regarding AI recommendation systems	0.001	Accepted
H2	Higher perceived anonymity of the Internet decreases the privacy concerns of users regarding AI recommendation systems	0.120	Rejected
H3	Higher perceived risk of data breaches increases the privacy concerns of users regarding AI recommendation systems	0.000	Accepted

H4	Higher perceived risk of consent issues increases the privacy concerns of users regarding AI recommendation systems	0.830	Rejected

Table 8 shows hypothesis results related to regression 1

4.5.2 Regression 2: Predicting Trust in AI Competence

The second regression was used to test H5. This regression was used to analyse the relationship between privacy concerns and trust in AI competence. The researcher used ordinal regression methods, and the following results were obtained.

4.5.2.1 Model fitting information.

The results for the model fitting checks in the second regression are as follows.

Model	-2Log likelihood	Chi-Square	Df	Sig
Intercept only	507.027			
Final	448.148	58.879	1	0.000
Link function: Logit				

Table 9 shows model fitting information for regression 2

The results above were used to check if the model fits well with the data. The test gave a p-value of 0.000, which is less than 0.05, which implies that the model fits well with the data.

4.5.2.2 Parameter estimates

The results for the parameter estimates are presented in the table below.

Variable	Parameter estimate	Std. error	Df	Sig.
PC	-1.1123	0.138	1	0.000

Table 10 shows regression coefficients for regression 2

The negative estimate of -1.1123 is statistically significant, with a p-value of 0.000. This result indicates that there is a significant inverse relationship between privacy concerns and trust in AI competence. Specifically, as privacy concerns decrease, trust in AI competence increases, which is consistent with the hypothesis.

The hypothesis results are presented in the table below

Code	Hypothesis	Sig	Result
H5	Higher privacy concerns decrease users' consumer trust in the competence of an AI system	0.000	Accepted

Table 11 shows hypothesis results related to regression 2

4.5.3 Regression 3: Predicting Trust in AI alignment.

The third regression is used to test H6. This regression analysis assesses the relationship between privacy concerns and trust in AI alignment. Ordinal regression analysis was used to make this prediction.

4.5.3.1 Model fitting checks.

Model	-2Log likelihood	Chi-Square	Df	Sig
Intercept only	473.565			
Final	468.853	4.713	1	0.030
Link function: Logit				

Table 12 shows model-fitting information for regression 3

The results above were used to check if the model fits well with the data. The test gave a p-value of 0.030, which is less than 0.05, which implies that the model fits well with the data.

4.5.3.2 Parameter estimates

Variable	Parameter estimate	Std. error	Df	Sig.
PC	-0.311	0.138	1	0.000

Table 13 shows regression coefficients for regression 3

The negative estimate of -0.311 is statistically significant, with a p-value of 0.000. This result indicates that there is a significant inverse relationship between privacy concerns and trust in Alignment. Specifically, as privacy concerns decrease, trust in AI Alignment increases, which is consistent with the hypothesis.

The hypothesis results are presented in the table below

Code	Hypothesis	Sig	Result
H6	Higher privacy concerns decrease users' trust in the system's alignment.	0.000	Accepted

Table 14 shows regression results related to regression 3

4.6 Discussion

The findings of this research study highlighted the positive role of perceived benefits of personalisation in reducing the level of privacy concerns. When users experience the advantages of personalisation, such as receiving recommendations tailored specifically to their preferences, their perceptions about data privacy tend to diminish. They begin to appreciate

the efficiencies such as relevant product suggestions and quicker access to information that meets their need. The findings align with the findings of the literature review that discusses the benefits of personalisation in enhancing user experience and satisfaction. Zanker et al. (2019) emphasised that personalised services increase user engagement, while Habil et al. (2023) highlighted the role of personalisation in fostering customer satisfaction and loyalty. This study's finding that personalisation reduces privacy concerns reinforces the idea that users are willing to trade some level of privacy for the perceived benefits of tailored experiences.

According to the findings of this research study, higher perceived anonymity of the Internet would decrease privacy concerns among users of AI recommendation systems. However, the findings were not significant since the p-value (0.120) was greater than 0.05. Therefore, this suggests that perceived anonymity would not necessarily reduce privacy concerns. This is consistent with a finding in the literature review that highlighted that sometimes, perceived anonymity of the Internet may be misleading and not align with reality (Hite et al., 2014). This is because technologies have allowed for practices such as data tracking, which can de-anonymise a user's presence on the Internet.

Another relevant finding of the research study is that higher perceived risks of data breaches would increase privacy concerns among users. This means that when users are aware of or believe there is a significant risk that their personal information could be exposed through a data breach, their concerns about privacy increase. The fear of sensitive data, such as financial details, being accessed by unauthorised parties leads to privacy concerns. These findings were consistent with findings in the literature review, such as Gao et al. (2021), who highlighted that the fear of data breaches could lead to changes in consumer behaviour, including reduced willingness to share personal information.

In addition, the findings of the research study stated that higher perceived risks of consent issues would increase privacy concerns. This highlights the critical role that user consent plays in influencing privacy concerns. When users believe that their consent is not adequately obtained, privacy concerns increase. These findings are consistent with findings in the literature review that consent is a critical factor in maintaining trust in AI systems (Ribeiro-Navarrete et al. (2021).

Additionally, the fifth hypothesis sought to investigate the effect of privacy concerns on trust in AI competence. The findings of the research study suggested that higher privacy concerns would decrease consumer trust in the competence of AI systems. The findings of the research study suggested that higher privacy concerns would decrease consumer trust in the competence of AI systems. When users have significant privacy concerns, they are likely to question the overall competence of the AI system itself. It is important to note that when privacy concerns are high, they create a barrier to trust. These findings connect with the findings in the literature review that highlight that trust in AI competence is essential for user acceptance of AI-driven recommendations (Manzini et al. (2024). With high privacy concerns, users are likely to question the system's ability to protect their personal information.

Furthermore, this research study explored the relationship between privacy concerns and trust in the alignment of AI systems with user values. The analysis confirmed this hypothesis, with a significant negative parameter estimate which had a p-value of 0.000, indicating that higher privacy concerns decrease trust in AI alignment. This finding is consistent with the literature, where alignment trust is seen as critical for long-term user engagement with AI systems. Gabriel and Ghazavi (2021) emphasised that users need to feel that AI systems operate ethically and align with their privacy expectations. The results suggest that when users are concerned about their privacy, they are less likely to trust that the AI system is aligned with their values.

5 CONCLUSIONS, LIMITATIONS AND RECOMMENDATIONS

5.1 Introduction

The research study sought to analyse how the usage of AI personalisation tools influences user's privacy concerns. The researcher conducted a literature review, which enabled them to establish relevant research variables. Thereafter, a research design was established whereby the researcher administered questionnaires to a sample of Amazon reviewers. Data was collected through the Lime survey tool, and data analysis was carried out through the SPSS statistical software. The previous chapter presented the results and made relevant discussions. This chapter summarises the findings made in the results chapter and makes key conclusions. In addition, this chapter presents the limitations of this research study as well as policy recommendations and recommendations for further research.

5.2 Summary of findings

This section describes the key findings of this research study. It is important to note that the theoretical framework used for this research was the privacy calculus theory. The privacy calculus theory posits that individuals engage in a cost-benefit analysis when deciding whether to disclose personal information in the online space. According to this theory, users weigh the perceived benefits of sharing their data against the potential privacy risks (Wang et al., 2024). If the perceived benefits outweigh the risks, users are more likely to share their personal information. On the other hand, if the risks are considered high, privacy concerns increase, which in turn may lead to reluctance to share data.

For this research study, the privacy calculus theory helped the researcher understand how perceived benefits and risks associated with AI-driven personalisation tools affect a user's privacy concerns. The perceived benefits in this case were personalisation and perceived anonymity of the Internet, while the perceived risks were data breaches and consent risks. The findings revealed that higher perceived benefits of personalisation lead to a significant decrease in privacy concerns. This supports the core premise of the privacy calculus theory, which suggests that when users perceive substantial advantages, they are more willing to tolerate potential privacy risks (Wang et al., 2024). In addition, the result did not find a significant relationship between perceived anonymity and privacy concerns, which is contrary to the expectations of the privacy calculus theory. This was attributed to the fact that data can be tracked, which makes the concept of perceived anonymity of the Internet invalid (Hite et

al., 2014). On the other hand, the findings of this research study implied that higher perceived risks increase the privacy concerns of an AI user. The findings of the research study concluded that when a user has a higher perception of a data breach, their privacy concerns would increase. In addition, if a user has a higher perception of consent risk, their privacy concerns would also increase.

In addition, the researcher further sought to investigate the impact of privacy concerns on trust. The trust was analysed in two dimensions: trust in AI competence and trust in AI alignment. Trust in AI competence is based on users' confidence that AI can handle tasks delegated to it efficiently and meet user expectations (Gieselmann & Sassenberg, 2023). If the user's privacy concerns are high, they may question the AI's ability to function correctly, which in turn may affect their perception of the system's ability to protect their data. On the other hand, trust in AI alignment was based on the belief that the AI system operates in ways that are consistent with users' ethical standards (Gabriel & Ghazavi, 2021). The findings of the research study suggested that higher privacy concerns reduce trust in AI alignment. When privacy concerns are high, users are less likely to trust that the AI system is aligned with their values, which, in turn, negatively affects their engagement levels.

5.3 Limitations of the research study

The research study effectively analyses the impact of AI-driven personalisation tools on privacy concerns and consumer trust. However, the research study has several limitations. The first limitation pertains to the research design that the researcher used to conduct the data collection and data analysis. The researcher exclusively used a quantitative research design in the methodology. While a quantitative research design is a powerful tool for generalising findings to larger populations, it can be limited to capturing the depth of respondent's perspectives regarding the subject matter. The use of a quantitative approach meant that data was primarily collected through structured questionnaires, which may not fully capture the subjective viewpoints on perceptions of AI-driven personalisation tools, privacy concerns and consumer trust.

Additionally, the research employed a cross-sectional design, which captures data at a single point in time. This approach limits the ability to assess changes in perceptions of the variables of interest over time since it only assesses current perceptions. It is important to note that perceptions of Privacy concerns and trust are not static. They can be influenced by various

factors that can evolve as users interact more with AI technologies and gain more experience. On the other hand, the cross-sectional design may also introduce bias, where the results are heavily influenced by a specific event that occurred during the time of data collection.

5.4 Recommendations

The researcher makes various recommendations both for practice and for further research. First and foremost, the researcher recommends the need for E-commerce platforms to be transparent in how they collect and use the data they collect from their AI-driven personalisation tools. This includes providing users with accessible explanations of data handling practices, privacy policies, and how AI systems operate. Transparency will go a long way in reducing the anxiety of data misuse and building customer trust levels in their AI recommendation systems.

In addition, the researcher recommends a mixed-method approach to this research topic that incorporates elements of qualitative and quantitative research approaches. The researcher recommends that other data collection methods should be used, such as interview discussions that will provide in-depth insight into underlying factors influencing privacy concerns and consumer trust. Qualitative insights can complement quantitative data by uncovering nuances and capturing the lived experiences of users, which are missed in the survey. Moreover, the researcher recommends the implementation of a longitudinal research study to track changes in the variables over time. This approach would allow researchers to analyse how privacy concerns and trust in AI-driven personalisation tools evolve due to shifts such as technology advancements, regulatory changes, or even user experiences.

6 REFERENCES:

Ahmed, G. (2021). Improving IoT privacy, data protection and security concerns. International Journal of Technology, Innovation and Management (IJTIM), 1(1).

Akhtar, N., Siddiqi, U. I., Islam, T., & Paul, J. (2022). Consumers' untrust and behavioral intentions in the backdrop of hotel booking attributes. International Journal of Contemporary Hospitality Management, 34(5), 2026-2047.

Altman, I. (1975). The Environment and Social Behaviour. Brooks/Cole.

Amaya, A., et al. (2021). New data sources in social science research: Things to know before working with Reddit data. Social science computer review, 39(5), 1-14.

Aslam, W., Hussain, A., Farhat, K., & Arif, I. (2020). Underlying factors influencing consumers' trust and loyalty in E-commerce. Business Perspectives and Research, 8(2), 186-204.

Balakrishnan, J., & Dwivedi, Y. K. (2021). Conversational commerce: Entering the next stage of AI-powered digital assistants. Annals of Operations Research.

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. International Journal of Information Management, 52, 102063.

Bandara, R., et al. (2020). Privacy concerns in E-commerce: A taxonomy and a future research agenda. Electronic Markets, 1-17.

Bauer, C., & Schiffinger, M. (2016). Perceived risks and benefits of online self-disclosure: Affected by culture? A meta-analysis of cultural differences as moderators of privacy calculus in person-to-crowd settings. https://core.ac.uk/download/pdf/301369784.pdf

Berg, T., et al. (2018). On the Rise of the FinTechs—Credit Scoring Using Digital Footprints. Federal Deposit Insurance Corporation Center for Financial Research Working Paper No. 2018-04.

Bhattacharya, S., Sharma, R. P., & Gupta, A. (2023). Does e-retailer's country of origin influence consumer privacy, trust and purchase intention?. Journal of Consumer Marketing, 40(2), 248-259.

Bjørlo, L., et al. (2021). The Role of Consumer Autonomy in Developing Sustainable AI: A Conceptual Framework. Sustainability, 13(2332).

Burger, A., & Silima, T. (2006). Sampling and sampling design. Journal of Public Administration, 41(3), 656–668.

Cappa, F., et al. (2021). Big data for creating and capturing value in the digitalised environment: Unpacking the effects of volume, variety, and veracity on firm performance. Journal of Product Innovation Management, 38(1), 49-67.

Chang, J., Wang, S. W., Mancini, C., McGrath-Mahrer, B., & Orama de Jesus, S. (2020). The complexity of cultural mismatch in higher education: Norms affecting first-generation college students' coping and help-seeking behaviors. Cultural Diversity and Ethnic Minority Psychology, 26(3), 280.

Chen, X., Sun, J., & Liu, H. (2022). Balancing web personalisation and consumer privacy concerns: Mechanisms of consumer trust and reactance. Journal of consumer behaviour.

Cheng, X., Hou, T., & Mou, J. (2021). Investigating perceived risks and benefits of information privacy disclosure in IT-enabled ride-sharing. Information & Management, 58(6), 103450

Choi, H. S. & Leon, S. (2023). When trust cues help helpfulness: investigating the effect of trust cues on online review helpfulness using big data survey based on the amazon platform. Electronic Commerce Research.

Cho, J., et al. (2010). Understanding the concept of privacy concerns: A review of literature. Journal of Privacy Studies, 5(2), 112-125.

Citron, D. K., & Solove, D. J. (2022). Privacy harms. BUL Rev., 2022.

Cooper, D. R., Schindler, P. S., & Sun, J. (2006). Business research methods (Vol. 9). McGrawhill New York.

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications

Dar, A. B., et al. (2020). Applicability of mobile contact tracing in fighting pandemic (COVID-19): Issues, challenges and solutions. Computer Science Review.

de Souza Pereira Moreira, G., et al. (2021, September). Transformers4rec: Bridging the gap between NLP and sequential/session-based recommendation. In Proceedings of the 15th ACM Conference on Recommender Systems (pp. 143-153).

Demirkan, S., et al. (2020). Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 7(2), 1-24.

Deng, H., Wang, W., & Lim, K. H. (2022). REPAIRING INTEGRITY-BASED TRUST VIOLATIONS IN ASCRIPTION DISPUTES FOR POTENTIAL E-COMMERCE CUSTOMERS.. MIS Quarterly.

Ding, Y., Ray, B., Devanbu, P., & Hellendoorn, V. J. (2020, December). Patching as translation: the data and the metaphor. In Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering (pp. 275-286).

Ebesu, T., et al. (2018). Collaborative memory network for Wang, X., & Chen, T. (2021). Analysis of the attributes of rights to inferred information and China's choice of legal regulation. Computer Law & Security Review.

Feng, J., et al. (2020). PMF: A Privacy-preserving Human Mobility Prediction Framework via Federated Learning. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 4(1), 10.

Gao, Y. L., et al. (2021). The effect of perceived error stability, brand perception, and relationship norms on consumer reaction to data breaches. International Journal of Hospitality Management.

Geradin, D., et al. (2020). GDPR Myopia: How a well-intended regulation ended up favoring Google in Ad Tech.

Ghoreishi, S. F. (2015). A review of trust in e-commerce. Journal of Electronic Commerce in Organizations, 13(2), 1-14.

Grabner-Kraeuter, S. (2002). The role of consumers' trust in online-shopping. Journal of Business Ethics, 39(1-2), 43-50.

Gu, Y., Ding, Z., Wang, S., & Yin, D. (2020, January). Hierarchical user profiling for e-commerce recommender systems. In Proceedings of the 13th International Conference on Web Search and Data Mining (pp. 223-231).

Guo, L. (2022). Cross-border e-commerce platform for commodity automatic pricing model based on deep learning. Electronic Commerce Research.

Gunasekar, S., et al. (2023). AI-enables product purchase on Amazon: what are the consumers saying?. foresight.

Ha, S. (2004). The role of consumer trust in online commerce. Journal of Business Research, 57(12), 136-144.

Ha, S., & Stoel, L. (2008). Consumer e-shopping acceptance: Antecedents in a technology acceptance model. Journal of Business Research, 61(7), 698-705.

Haleem, A., et al. (2022). Artificial intelligence (AI) applications for marketing: A literature-based study. International Journal of Intelligent Networks.

Hathaliya, J. J., & Tanwar, S. (Year). An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications.

He, M., Qin, J., Wen, M., & Chen, W. (2021). Sustaining consumer trust and continuance intention by institutional mechanisms: An empirical survey of DiDi in China. IEEE Access.

Hermès, S., et al. (2020). The digital transformation of the healthcare industry: Exploring the rise of emerging platform ecosystems and their influence on the role of patients. Business Research, 13, 1033-1069.

Himeur, Y., et al. (2022). Latest trends of security and privacy in recommender systems: A comprehensive review and future perspectives. Computers & Security, 118, 1-16.

Jabareen, Y. (2009). Building a Conceptual Framework: Philosophy, Definitions, and Procedure. International Journal of Qualitative Methods, 8(4), 49–62. https://doi.org/10.1177/160940690900800406

Jarek, K., & Mazurek, G. (2019). Artificial intelligence and the future of marketing. Journal of Marketing Management, 35(7-8), 693-699.

Javed, U., Shaukat, K., Hameed, I. A., Iqbal, F., Alam, T. M., & Luo, S. (2021). A review of content-based and context-based recommendation systems. International Journal of Emerging Technologies in Learning (iJET), 16(3), 274-306.

Jones, R. (2019). AI and the future of privacy. International Data Privacy Law, 9(1), 36-48.

Kaushal, V., & Yadav, R. (2022). The role of chatbots in academic libraries: An experience-based perspective. Journal of the Australian Library and Information Association, 71(3), 215-232.

Karavidaj, J. (2020). A Comparative Analysis of Memory-based and Model-based Collaborative Filtering Methods for myAnime Recommendations Systems.

Khan, I. A. (2015). Ethical considerations in an educational research: A critical analysis. British Journal of Education, Society & Behavioural Science, 13(2), 1–8.

Khatoon, S., & Rehman, V. (2021). Negative emotions in consumer brand relationship: A review and future research agenda. International Journal of Consumer Studies, 45(4), 719-749.

Kim, D. J., et al. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Systems, 44(2), 544-564.

Kim, B., & Kim, D. (2020). Understanding the key antecedents of users' disclosing behaviors on social networking sites: The privacy paradox. Sustainability, 12(12), 5163.

Klaus, P., & Zaichkowsky, J. (2020). AI voice bots: A services marketing research agenda. Journal of Services Marketing.

Ko, H., et al. (2022). A survey of recommendation systems: Recommendation models, techniques, and application fields. Electronics, 11(15), 2306.

Kumar, N., & Kumar, R. (2021). The application of artificial intelligence in electronic commerce. Turkish Journal of Computer and Mathematics Education, 12(12), 1679-1682.

Kumar, V., et al. (2019). Understanding the role of artificial intelligence in personalised engagement marketing. California Management Review, 61(4), 135-155.

Lankton, N. K., McKnight, D. H., & Tripp, J. F. (2019). Understanding the antecedents and outcomes of Facebook privacy behaviors: An integrated model. IEEE Transactions on Engineering Management, 67(3), 697–711.

Lari, H. A., et al. (2022). Artificial Intelligence in E-commerce: Applications, Implications and Challenges. Asian Journal of Management.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of Social Issues, 33(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lee, J. K., Chang, Y., Kwon, H. Y., & Kim, B. (2020). Reconciliation of privacy with preventive cybersecurity: The bright internet approach. Information Systems Frontiers.

Lee, S. Y. (2020). The age of consumer distrust: exploring the role of consumer expectations and brand crisis in the formation of brand distrust.

Li, B., Yin, Z., Ding, J., Xu, S., Zhang, B., Ma, Y., & Zhang, L. (2020). Key influencing factors of consumers' vegetable e-commerce adoption willingness, behavior, and willingness-behavior consistency in Beijing, China. British Food Journal, 122(12), 3741-3756.

Li, S., et al. (2021). Research and analysis of an enterprise E-commerce marketing system under the big data environment. Journal of Organizational and End User Computing (JOEUC), 33(4), 54-71.

Li, X., et al. (2021). Privacy-preserving deep learning model against poisoning attacks in E-commerce. IEEE Transactions on Information Forensics and Security, 17(6), 1214-1229.

Li, X., et al. (2020). Scalable Collaborative Filtering with Jointly Derived Neighborhood Interpolation Weights. IEEE Transactions on Knowledge and Data Engineering, 33(5), 2035-2048.

Li, Y., et al. (2020). Deep learning-based recommendation in E-commerce. Knowledge-Based Systems, 194, 105616.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. Decision Support Systems, 54(1), 471–481.

Liang, C., et al. (2022). An investigation of consumers' continuance intention towards voice commerce. Electronic Commerce Research and Applications, 57, 100995.

Lim, Y. G., et al. (2020). E-commerce platform selection: A comprehensive review. Journal of Internet Commerce, 19(2), 107-137.

Lin, X. & Wang, X. (2023). Towards a model of social commerce: improving the effectiveness of e-commerce through leveraging social media tools based on consumers' dual roles. European Journal of Information Systems.

Liu, Y., et al. (2020). A survey on augmented reality in E-commerce: Perspectives from both practitioners and researchers. IEEE Access, 8, 53653-53671.

Liu, L. (2016). Using generic inductive approach in qualitative educational research: A case study analysis. Journal of Education and Learning, 5(2), 129–135.

Lnenicka, M. & Nikiforova, A. (2021). Transparency-by-design: What is the role of open data portals?. Telematics and Informatics.

Luo, Y., et al. (2022). A hybrid recommendation approach for E-commerce using neural collaborative filtering and feature engineering. Applied Sciences, 12(4), 1808.

Maheshwari, P., et al. (2020). Predictive modeling and recommendation system for E-commerce. Journal of Retailing and Consumer Services, 54, 1-12.

Majumdar, A., & Garg, L. (2021). A system for secure and private health data exchange using blockchain. IETE Journal of Research.

McLean, G., et al. (2020). Towards more fair and interpretable Recommender Systems: New research directions. 13th ACM Conference on Recommender Systems (RecSys 2019).

Micheli, M., & Rodan, S. (2019). A brief history of artificial intelligence. ACM Computing Surveys (CSUR), 52(4), 1-38.

Miesler, L., et al. (2021). Product recommendation in social commerce: An empirical study on the determinants of consumers' acceptance of product recommendations on Facebook. Electronic Commerce Research and Applications, 50, 101023.

Min, J., & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. Journal of the Association for Information Science and Technology, 66(4), 839–857. https://doi.org/10.1002/asi.23206

Montecchiani, F., et al. (2021). Trust in digital platforms: Literature review and directions for future research. Journal of the Association for Information Systems, 22(6), 1345-1382.

Morris, D. (2021). Digital Preservation: Keeping Knowledge Alive. Journal of Electronic Resources Librarianship, 33(2), 74-88.

Natarajan, S., et al. (2022). The effects of blockchain technology on healthcare: An overview. Journal of Ambient Intelligence and Humanized Computing.

Nafsi, F. A. (2023). Ethical Considerations In Conducting Research For Thesis: Students' Beliefs And Practices [PhD Thesis, UIN Ar-Raniry Fakultas Tarbiyah dan Keguruan]. https://repository.ar-raniry.ac.id/id/eprint/25699/

Nguyen, D. T., et al. (2022). The future of blockchain in electronic commerce: Research directions and opportunities. Electronic Commerce Research.

Ning, L., et al. (2021). Research on Privacy Protection of Electronic Commerce Personal Information Based on Blockchain. In 2021 2nd International Conference on E-Commerce, E-Business and E-Government (ICEEG 2021) (pp. 18-23). ACM.

Pappa, G. L., et al. (2021). Blockchain technologies in online voting systems: A comprehensive review. Journal of Network and Computer Applications, 175, 102952.

Paul, J., et al. (2021). Consumers' privacy concerns and associated protection measures in Internet of things (IoT)-enabled smart homes: A thematic analysis. Journal of Consumer Affairs, 55(2), 491-516.

Pires, M. B., et al. (2021). A blockchain-based solution for enhancing patient privacy in electronic health records. Journal of Medical Systems, 45(1), 1-9.

Ponnurangam, D., et al. (2021). Enhancing E-commerce sales through AI-based personalisation. Journal of Theoretical and Applied Electronic Commerce Research, 16(10), 1-16.

Portillo, F., et al. (2022). Understanding trust in electronic commerce: A literature review and research agenda. Computers in Human Behavior, 121, 106-119.

Qaiser, N., et al. (2020). Big data analytics in E-commerce: A systematic review and agenda for future research. Electronic Commerce Research and Applications, 40, 100904.

Qin, L., Qu, Q., Zhang, L., & Wu, H. (2021). Platform trust in C2C e-commerce platform: The sellers' cultural perspective. Information Technology and Management.

Raghavendra, S. P., et al. (2021). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. Sustainable Cities and Society, 75, 103336.

Rakić, S., et al. (2020). A critical review of blockchain and its current applications. IEEE Access, 8, 210134-210151.

Ramya, A., et al. (2021). Deep learning approaches for click-through rate prediction: Challenges and opportunities. Artificial Intelligence Review, 54(1), 429-463.

Rao, A. S., et al. (2022). The implications of blockchain for sustainable supply chain management: A systematic literature review. Journal of Cleaner Production, 337, 1301-1318.

Ribeiro, M. T., et al. (2020). Beyond accuracy: Behavioral testing of NLP models with CheckList. In Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics (pp. 4902-4912).

Rich, S. J., et al. (2021). The State of AI Ethics Report (2021): Why Ethics Matters in Artificial Intelligence. Montreal AI Ethics Institute.

Rodrigues, C. M., et al. (2022). Voice shopping: A survey and research directions. Information Processing & Management, 59(2), 102858.

Rodrigues, D. M., et al. (2020). Trust in E-commerce: A bibliometric analysis. Scientometrics, 124(2), 1269-1296.

Rzepka, C., Berger, B., & Hess, T. (2020). Why another customer channel? Consumers' perceived benefits and costs of voice commerce.

Sandfeld, M., et al. (2022). Overcoming information asymmetry with AI in E-commerce: the role of personalised product recommendations. Journal of Business Research.

Saravanan, M., et al. (2020). A comprehensive review on IoT-based healthcare applications and its security challenges. Journal of Ambient Intelligence and Humanized Computing.

Saunders, M. N., Lewis, P., Thornhill, A., & Bristow, A. (2015). Understanding research philosophy and approaches to theory development. https://oro.open.ac.uk/53393/

Schöning, J., et al. (2022). Factors affecting the public perception of artificial intelligence: A systematic review. Frontiers in Psychology, 13, 806946.

Sharma, P., et al. (2021). Artificial intelligence in E-commerce: A systematic literature review and bibliometric analysis. Journal of Retailing and Consumer Services, 63, 102706.

Shi, Z., et al. (2021). A survey of deep learning techniques for E-commerce recommendation. Future Generation Computer Systems, 115, 31-47.

Srinivasan, A., et al. (2022). Understanding the influence of Artificial Intelligence (AI) in online customer engagement: A structured literature review and research agenda. Information & Management, 59(1), 103474.

Srivastava, S., et al. (2021). Blockchain technology in the Indian automotive industry: A review, recent developments, and future directions. Computers & Industrial Engineering, 159, 107483.

Soni, V. D. (2020). Emerging Roles of Artificial Intelligence in Ecommerce. CompSciRN: Artificial Intelligence (Topic). https://api.semanticscholar.org/CorpusID:225776354

Su, Z., et al. (2020). Context-aware recommendation with hierarchical tensor factorisation. Knowledge-Based Systems, 195, 105660.

Sun, J., et al. (2020). A review of machine learning and artificial intelligence in recommendation systems. Journal of Management Analytics, 7(2), 197-215.

Sundararajan, A., et al. (2021). On the impact of blockchain technology on healthcare privacy. IEEE Transactions on Network and Service Management, 18(4), 2563-2577.

Sunstein, C. R. & Vermeule, A. (2021). The Unitary Executive: Past, Present, Future. The Supreme Court Review.

Suresh, M., et al. (2022). Understanding the privacy paradox in the context of e-commerce apps: An empirical investigation. Journal of Retailing and Consumer Services, 67, 102869.

Taherdoost, H. (2016). Sampling methods in research methodology; how to choose a sampling technique for research. How to Choose a Sampling Technique for Research (April 10, 2016). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3205035

Tang, Y., Zhang, Y., & Ning, X. (2023). Uncertainty in the platform market: the information asymmetry perspective. Computers in Human Behavior.

Tian, Y., Zhang, H., Jiang, Y., & Yang, Y. (2022). Understanding trust and perceived risk in sharing accommodation: An extended elaboration likelihood model and moderated by risk attitude. Journal of Hospitality Marketing & Management, 31(3), 348-368.

Tung, F. Y., et al. (2020). Understanding consumers' continuance intentions toward voice shopping. Journal of Interactive Marketing, 52, 56-72.

Upadhyay, N., et al. (2021). A comprehensive review on blockchain technology in healthcare sector. Journal of King Saud University-Computer and Information Sciences.

Wang, R., Bush-Evans, R., Arden-Close, E., Bolat, E., McAlaney, J., Hodge, S., ... & Phalp, K. (2023). Transparency in persuasive technology, immersive technology, and online marketing: Facilitating users' informed decision making and practical implications. Computers in Human Behavior, 139, 107545.

Wang, W., Kumar, N., Chen, J., Gong, Z., Kong, X., Wei, W., & Gao, H. (2020). Realising the potential of the Internet of things for smart tourism with 5G and AI. IEEE network, 34(6), 295-301.

Wang, X., et al. (2020). A review on trust management for online social commerce: Taxonomy, elements, antecedents, and consequences. IEEE Access, 8, 126220-126240.

Wang, Y., et al. (2020). Security and privacy in E-commerce: A comprehensive study. IEEE Access, 8, 178892-178917.

Wang, B., Liu, Y., Qian, J., & Parker, S. K. (2021). Achieving effective remote working during the COVID-19 pandemic: A work design perspective.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. International Journal of Information Management, 36(4), 531–542.

Warburg, R. J., et al. (2020). Applying big data analytics to electronic commerce data: A literature review. Journal of Big Data, 7(1), 1-31.

Wilson, D. W. (2015). Overcoming information privacy concerns: Learning from three disclosure contexts. The University of Arizona. https://search.proquest.com/openview/2e8c854116d9f703896fb04ee59edd5a/1?pq-origsite=gscholar&cbl=18750

Wu, D., et al. (2020). Artificial intelligence in E-commerce: A systematic literature review. Technological Forecasting and Social Change, 151, 119855.

Wu, K., & Chi, K. (2023). Enhanced e-commerce customer engagement: A comprehensive three-tiered recommendation system. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(3), 348-359.

Xiong, W., et al. (2020). Convolutional Poisson Matrix Factorization. In Advances in Neural Information Processing Systems (Vol. 33).

Xu, G., et al. (2021). Building user trust in AI: A cross-domain trust prediction model. Journal of the Association for Information Science and Technology, 72(6), 660-678.

Xu, Y., & Wang, D. (2023). Privacy Concerns and Antecedents of Building Data Sharing: A Privacy Calculus Perspective. ACM SIGEnergy Energy Informatics Review, 3(2), 3–18. https://doi.org/10.1145/3607114.3607116

Yan, B., Zhang, X., Wu, L., Zhu, H., & Chen, B. (2020). Why do countries respond differently to COVID-19? A comparative study of Sweden, China, France, and Japan. The American review of public administration, 50(6-7), 762-769.

Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access

Yasin, W., Harimoorthy, K., & Vetriveeran, D. (2023). Identification of Consumer Buying Patterns using KNN in E-Commerce Applications. 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), 187–192. https://ieeexplore.ieee.org/abstract/document/10266130/

Young, M., Varpio, L., Uijtdehaage, S., & Paradis, E. (2020). The spectrum of inductive and deductive research approaches using quantitative and qualitative data. Academic Medicine, 95(7), 1122.

Yordanova, K., et al. (2022). The impact of artificial intelligence and machine learning on the future of marketing. Journal of Business Research, 142, 234-243.

Yu, H., et al. (2021). A review of hybrid recommendation systems based on deep learning. Knowledge-Based Systems, 219, 106935.

Zhang, J., et al. (2022). AI in E-commerce: A comprehensive review and research directions. Information Systems Frontiers, 24(1), 95-119.

Zhang, Q., Lu, J., & Jin, Y. (2021). Artificial intelligence in recommender systems. Complex & Intelligent Systems.

Zhang, R., Fang, L., He, X., & Wei, C. (2023). Controlling Credit Risk in E-commerce. In The Whole Process of E-commerce Security Management System: Design and Implementation (pp. 225-260). Singapore: Springer Nature Singapore.

Zhang, Y., et al. (2021). Building brand trust in E-commerce: The role of AI recommender systems. Journal of Electronic Commerce Research, 22(2), 94-115.

Zhang, J., Hassandoust, F., & Williams, J. E. (2020). Online customer trust in the context of the general data protection regulation (GDPR). Pacific Asia Journal of the Association for Information Systems, 12(1), 4.

Zhao, Y., Wang, L., Tang, H., & Zhang, Y. (2020). Electronic word-of-mouth and consumer purchase intentions in social e-commerce. Electronic Commerce Research and Applications, 41, 100980.

Zhao, Y., Wang, N., Li, Y., Zhou, R., & Li, S. (2021). Do cultural differences affect users'e-learning adoption? A meta-analysis. British Journal of Educational Technology, 52(1), 20-41.

Zhu, Y. Q. & Kanjanamekanant, K. (2021). No trespassing: Exploring privacy boundaries in personalised advertisement and its effects on ad attitude and purchase intentions on social media. Information & Management

7 APPENDIX

7.1 Appendix 7.1

Communalities

	Initial	Extraction
PS1	1.000	.652
PS2	1.000	.598
PS3	1.000	.550
PS4	1.000	.632
PA1	1.000	.421
PA2	1.000	.711
PA3	1.000	.646
PA4	1.000	.647
DB1	1.000	.570
DB2	1.000	.670
DB3	1.000	.721
DB4	1.000	.659
CR1	1.000	.453
CR2	1.000	.611
CR3	1.000	.622
CR4	1.000	.493

Extraction Method: Principal Component Analysis.

7.2 Appendix 7.2

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.797
Bartlett's Test of Sphericity	Approx. Chi-Square	1309.932
	df	78
	Sig.	.000

7.3 Appendix 7.3

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %

1	3.933	30.255	30.255	3.933	30.255	30.255	
2	2.246	17.275	47.530	2.246	17.275	47.530	
3	1.400	10.767	58.297	1.400	10.767	58.297	
4	1.091	8.391	66.687	1.091	8.391	66.687	
5	.710	5.460	72.147				
6	.611	4.696	76.843				
7	.562	4.321	81.164				
8	.505	3.887	85.051				
9	.484	3.723	88.773				
10	.405	3.115	91.888				
11	.378	2.907	94.794				
12	.361	2.780	97.574				
13	.315	2.426	100.000				

Extraction Method: Principal Component Analysis.

7.4 Appendix 7.4

Rotated Component Matrix[a]

	Component			
	1	2	3	4
PS1	.802			
PS2	.752			
PS3	.692			
PS4	.771			
PA2			.816	
PA3			.816	
PA4			.833	
DB1		.667		
DB2		.752		
DB3		.845		
DB4		.798		
CR2				.763
CR3				.859

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.[a]

a. Rotation converged in 5 iterations.

7.5 Appendix 7.5

Communalities

	Initial	Extraction

TC1	1.000	.642
TC2	1.000	.653
TC3	1.000	.625
TC4	1.000	.573
TA1	1.000	.547
TA2	1.000	.544
TA3	1.000	.689
TA4	1.000	.387

Extraction Method: Principal Component Analysis.

7.6 Appendix 7.6

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.749
Bartlett's Test of Sphericity	Approx. Chi-Square	592.290
	df	21
	Sig.	.000

7.7 Appendix 7.7

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.888	41.264	41.264	2.888	41.264	41.264
2	1.502	21.461	62.725	1.502	21.461	62.725
3	.674	9.631	72.356			
4	.607	8.672	81.028			
5	.550	7.857	88.885			
6	.419	5.988	94.873			
7	.359	5.127	100.000			

Extraction Method: Principal Component Analysis.

7.8 Appendix 7.8

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
PS	.239	313	.000	.801	313	.000
PA	.144	313	.000	.919	313	.000
DB	.219	313	.000	.853	313	.000

CR	.163	313	.000	.960	313	.000
PC	.215	313	.000	.854	313	.000
TC	.168	313	.000	.916	313	.000
TA	.131	313	.000	.971	313	.000

a. Lilliefors Significance Correction

7.9 Appendix 7.9

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Log_PS	.268	313	.000	.680	313	.000
Log_PA	.101	313	.000	.978	313	.000
Log_DB	.256	313	.000	.735	313	.000
Log_CR	.177	313	.000	.920	313	.000
Log_PC	.254	313	.000	.711	313	.000
Log_TC	.196	313	.000	.794	313	.000
Log_TA	.166	313	.000	.929	313	.000

a. Lilliefors Significance Correction