Solo International Collaboration and Publication of Social Sciences and Humanities
E-ISSN: 2988-3512
Vol.4, No.1, 2026, pp. 347-360
DOI: https://doi.org/10.61455/sicopus.v4i01.445

Data Privacy and Business Performance of E-commerce Industry: Towards Cybersecurity through Transparency and Control

***Priya Sukrirthanandan*[1], *Salman Sarwar*[2], *Sana Ashraf*[3]**

[1]Faculty of Business Technology, University of Cyberjaya, Malaysia

[2]Faculty of Business, Salar International University, Pakistan

[3]Faculty of Business & Finance, Lahore Leads University, Pakistan

[1]priya@cyberjaya.edu.my, [2]salmansarwar333@gmail.com,
[3]phd_ms_salman@pakaims.edu.pk

Received August 28, 2025; Revised November 29, 2025; Accepted December 25, 2025

Abstract

Objective: A crucial element of the modern digital ecosystem is data privacy. A comparable viewpoint is seen in the realm of e-commerce, which has emerged as the primary economic engine on a global scale. The growth in the consumer base and the sheer quantity of data being transferred within the e-commerce platforms constitute a serious risk. In compliance with international regulations, e-commerce platforms are implementing data privacy rules that include transparent and control-centric processes. **Theoretical framework:** The current study explored how Malaysian e-commerce enterprises' commercial performance is fueled by data privacy rules' control and transparency components. A two-pronged approach was taken in conducting the research using qualitative and quantitative methodology. **Literature review:** First, the transparency and control features of the data privacy policies of a chosen group of e-commerce enterprises were qualitatively benchmarked. The findings indicated that while Carousell, Ezbuy, and Mudah are some of the e-commerce companies with low levels of transparency and control practices, **Methods:** Lazada and Shopee have the highest levels of transparency and control practices within their data privacy policies. Subsequently, the analysis was further triangulated with a quantitative analysis from 379 respondents. The data processing and results indicate the increased transparency & control of data privacy policy practices for business performance of e-commerce companies. It includes the internal, performance, and practice benchmarking for e-commerce platforms operating in Malaysia. **Results:** There is specific stress on the transparency and control sections of data privacy for each of the e-commerce platforms operating in Malaysia. **Implications:** This research recommends the transparent and controlled review of the data privacy policies on the e-commerce platforms for effective communication, privacy, and behavioral business decisions. **Novelty**: the study will help setting corporate digital business to ensure cybersecurity and trust of the customer in Malaysia. The serious concern of customer digital information is aptly and rightly channeled to make further customer satisfied. The study output will help policy makers to enhance business with the trust of the customer for the obtained information.

Keywords: data privacy, transparency, business performance, cybersecurity, digital resilience.

INTRODUCTION

In the digital age, cybersecurity has emerged as a critical global concern, deeply intertwined with national security, economic stability, and the protection of individual rights. As nations, businesses, and individuals become increasingly dependent on digital infrastructure, the threat landscape continues to evolve, exposing vulnerabilities that have far-reaching consequences. From state-sponsored cyber operations and cybercrime networks to ransomware attacks and critical infrastructure breaches, the scale and sophistication of cyber threats are unprecedented. These developments have not only highlighted the fragility of global cyberspace but have also underscored the need for comprehensive governance mechanisms that can address the complexities of cybersecurity in an interconnected world [1].

The rapid expansion of cyberspace has outpaced the evolution of legal and regulatory systems. While various domestic laws and regional agreements attempt to mitigate cyber threats, the transnational nature of cyber activities poses unique challenges that require cooperation beyond national borders. Issues such as attribution of cyberattacks, jurisdictional conflicts, and the application of international legal norms in cyberspace remain unresolved. As a result, the role of international law in regulating cybersecurity has become a focal point of academic and policy debate. The absence of a binding and universally accepted international legal framework exacerbates the legal uncertainty surrounding state behavior in cyberspace, particularly in cases involving cyber espionage, cyber warfare, and interference in domestic affairs [2].

The research on data privacy and practice areas of transparency and control are trending areas from last few decades. Using the data, individuals highly rely on reasoning approaches such as experience, theory, and preconceptions that are primarily influenced by personal prejudice to investigate and discover the law of unknowns [3]. Nevertheless, today the use of information and communication technology (ICT) has changed society's style and habits. Society is witnessing explosive data growth due to the rapid evolution of technology and network mechanisms [4]. Privacy pertains to the safeguarding of personal data or information and can be described as the extent to which an individual permits the sharing of their data or information with external entities [5].

The recent technological development and progress, in conjunction with the scientific advancements and the increased reliance on technology, have brought the issue of national security to the forefront of concerns [6]. In addition, it highlights the numerous obstacles that both developed and developing countries have in their efforts to counteract cyber threats and to increase awareness about the inherent risks that are linked with technology. In summary, given that we are living in an age of information, the issue of privacy is the most pressing concern of our day [7]. As information and communication technology (ICT) systems continue to spread, users' privacy must be taken into consideration and protected. This is a notable concern.

The internet age has dramatically revolutionized the pace of innovation, value generation, and monetization. It is not a far-fetched prediction that more than half of the world's population is connected to the internet [8]. As access to the internet is deemed a core human right, it is favorable for the contemporary digitized era. This includes the customers' mistrust of data privacy, which has increased due to persistent data breaches, disputes among businesses and service providers over cookies, wallet approaches, and continuous misinformation [9].

The following research questions are posed: -

RQ1: What are the data privacy policies' transparency practices by e-commerce companies in Malaysia?

RQ2: What are the data privacy policies and control practices of e-commerce companies in Malaysia?

E-ISSN: 2988-3512

RQ3: What is the impact of data privacy policy's transparency (private information boundary and private information control) and control (private information rules, private information co-ownership, and boundary turbulence) on the business performance of e-commerce companies in Malaysia?

Nowadays, digital data privacy & Cybersecurity is a nascent and rapidly growing priorities in Malaysia; thus, this study will be significant for the Malaysian government as the e-commerce industry notably impacts the nation's income. As stated, businesses highly value the data gathered from their customers as this action enables them to send out targeted promotions, forecast sales patterns, and enhance their product quality. However, some consumers believe that data collection is an invasion of their privacy and a practice that can be misused, resulting in the distrust and suspicion of some businesses. As a result, this study aims to prove the essence of including transparency and control elements in the data privacy policy of the nation [10].

This study aims to examine the influence of data privacy policies' transparency and control elements on the business performance of e-commerce firms in Malaysia.

LITERATURE REVIEW

Communication Privacy Management Theory (CPM)

Data privacy remains a vital issue for consumers, despite the increasing use of e-commerce [11]. As claimed, privacy is people's ability to decide when, how, and to what extent their personal data can be disseminated to external parties [12]. Therefore, CPM addresses the uncertainty between data exposure and privacy by investigating how and why individuals decide to reveal their private information across various contexts [13]. As cited by, CPM can be used as a theory in order to address the questions regarding the management and control of personal data, as well as the rejection or allowance of access to that information [14].

In essence, individuals have the control and decision-making power to disclose their personal data. As a result, the consideration of revealing data/information is what Sandra Petronio examined in the CPM theory. In other words, this theory aims to implicate the decision-making process in revealing or restricting private information in building a relationship [15].

The reason for choosing this theory as one of the underpinning theories of the present study is that CPM relies on multiple assumptions, such as prioritizing private information rights, defining personal boundaries between private and public data, and the rules of private information in controlling data privacy management. Similarly, also noted that the CPM consists of three significant elements, namely privacy rights, control, and turbulence [16]. Accordingly, CPM theory provides a paradigm for comprehending the dual process of releasing or concealing consumers' data, while this theory is also deemed a map that enables individuals to navigate privacy [17].

Communication Privacy Management (CPM) theory and data privacy

The application of Communication Privacy Management (CPM) theory to the preservation of digital data privacy & Cybersecurity is of the utmost significance within the framework of the rapidly changing environment of the e-commerce company. This is because CPM theory was developed to safeguard the privacy of digital data. When it comes to the manner in which individuals actively manage their personal information, particularly within the complex dynamics of e-commerce transactions, this theoretical approach, which has its roots in the foundational work of [18], provides valuable insights that can be utilized.

E-ISSN: 2988-3512

The constant exchange of personal information is one of the factors that adds to the palpable concerns that customers have regarding the privacy of their data in the realm of e-commerce, which is conducted online [19]. The CPM theory, which is founded on the idea that individuals can exercise active control over the sharing of their private data, is particularly pertinent in terms of recognizing and resolving these difficulties. A strong emphasis is placed on the establishment and assertion of privacy limits within the framework. This is accomplished by viewing users as proactive agents who are navigating their own privacy problems for themselves.

Behavioral Decision Theory (BDT)

The decision-making process of consumers is a dynamic behavior [20]; however, the factors of e-commerce intention and online choice behavior can be determined [21].

According to the Behavioral Decision Theory (BDT) that was proposed by Ward Edwards in 1954, consumer decisions are significantly impacted by their values and beliefs. This is because consumers in today's digitized era demand more transparency and control over their personal data and information. This is because privacy continues to be an essential component of trust [22], which in turn affects their decision-making process. Furthermore, concurred with the notion that businesses should make available a user-friendly gateway that gives data subjects the ability to exercise control over their data. This is because failing to offer customers essential access to data and information can hurt business performance by causing customers to lose trust in the company [23].

The regulation of cybersecurity through international law is a complex yet indispensable endeavor. While there have been notable efforts to establish legal norms and cooperative frameworks, significant challenges remain in terms of legitimacy, enforcement, and global consensus. This research begins by setting the context of cybersecurity’s growing importance and the inherent challenges it presents to international legal systems. It then delves into the foundational question of the extent and efficacy of international law in governing cyberspace, ultimately seeking to identify pragmatic pathways for strengthening global cybersecurity through legal innovation and multilateral collaboration [24].

One of the most prominent international treaties related to cybersecurity is the Budapest Convention on Cybercrime, adopted by the Council of Europe in 2001. It is the first and, so far, the only legally binding international treaty that seeks to harmonize national laws, enhance investigative techniques, and improve international cooperation in combating cybercrime. The Convention criminalizes various cyber activities, such as illegal access to systems, data interference, and the misuse of devices. It also includes provisions for mutual legal assistance among signatories, which is critical in cross-border cyber investigations [25]. However, the Budapest Convention has been criticized for its limited global reach. Many countries, including key cyber powers like Russia and China, have not signed the treaty, citing concerns over sovereignty, data sharing, and the perceived Western-centric nature of its provisions. As a result, while the Convention provides a valuable legal foundation for combating cybercrime, its effectiveness is constrained by geopolitical divisions and the absence of universal participation.

In addition to formal treaties, customary international law plays an increasingly important role in regulating state conduct in cyberspace. Customary law emerges from consistent state practice accompanied by a belief that such practice is legally required (opinio juris). In the context of cybersecurity, several principles of customary international law are being tested and, in some cases, slowly solidified. For example, the prohibition of the use of force, the principle of non-intervention in the internal affairs of other states, and the obligation to prevent harm emanating from one's territory are all potentially applicable to cyberspace [26].

However, the application of these norms to cyber operations is far from settled. States vary widely in how they interpret and apply these principles in the cyber context. For instance, while one state may view a cyberattack on its financial system as a use of force, another may

E-ISSN: 2988-3512

interpret it as a mere inconvenience not rising to the level of an armed attack. This lack of uniformity poses significant challenges to the development of a coherent body of customary international law in cybersecurity. Nevertheless, the accumulation of state responses to cyber incidents and their articulation of legal justifications are gradually contributing to the clarification of how traditional norms apply in this new domain [27].

E-commerce is an ever-evolving business space that has continued to change the way business and commerce are facilitated today. In general, the virtual space unavoidably shapes both national and international economies; Malaysia's e-commerce landscape proliferates yearly with an annual growth rate of approximately 24% [28]. Nevertheless, the Covid-19 pandemic has fueled the electronic commerce industry in Malaysia, which is known as a nation with an attractive market for e-commerce in Southeast Asia due to its dynamic economy and well-established infrastructure for digital technologies.

Malaysia's income generated from e-commerce has amounted to RM279 billion due to an increasing trend during the nationwide lockdown (MCO) [29]. According to the Digital Economy Report 2021, publicized by the Department of Statistics Malaysia (DOSM), the e-commerce income for the first nine months (January to September) was RM801.2 billion, a growth of 23.1% year on year, with Selangor, Kuala Lumpur, Johor, and Penang leading the path.

The literature review in this template refers to previous studies, which have been adapted and modified by the creator to ensure novelty and distinctiveness. Theories about the studies or themes studied and relevant previous research.

METHODOLOGY

The role of trust is paramount in a dynamic process. Consumers are more likely to engage with e-commerce platforms that they trust to handle their personal information responsibly. Trust is not static; it is built and reinforced through transparent communication, ethical data practices, and a track record of secure transactions. Equally, any breach of trust, such as a data mishandling incident, can lead to a rapid erosion of consumer confidence. The decision-making process is also influenced by the perceived benefits and risks associated with data sharing. Consumers weigh the convenience and personalized experiences offered by e-commerce platforms against the potential risks of privacy infringement. E-commerce businesses that can clearly articulate the value proposition and demonstrate the security measures in place are more likely to align with consumer expectations. The regulatory landscape plays a crucial role in shaping the dynamics of consumer decision-making. Data protection laws, such as the General Data Protection Regulation (GDPR) and other regional or industry-specific regulations, set standards for how personal information should be handled. Consumers often consider the compliance of e-commerce platforms with these regulations as an indicator of their commitment to data privacy and ethical conduct.

Sequential Exploratory Design

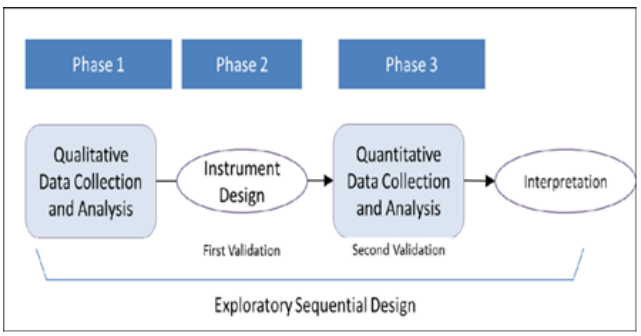


Figure 1. Sequential Exploratory Design

Source: Sequential Exploratory Design (Creswell & Clark, 2011)

Quantitative and qualitative research methodologies have long been viewed as conflicting paradigms [30]; however, there have been attempts called mixed methods to incorporate both as complementary instead of contending methods [31]. In general, studies involving systematic and impartial analysis of numerical data use the quantitative method, while any research that initially determines and defines an area of interest that results in the formulation of the hypotheses is referred to as qualitative research. Nonetheless, the principal differences between qualitative and quantitative studies that numerous scholars have long debated will be comprehensively discussed in the following sections.

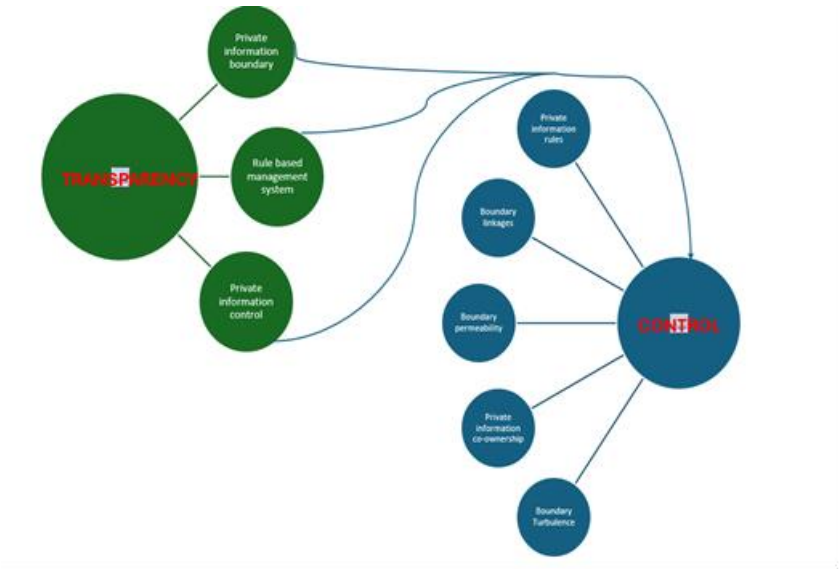
One way to measure the data privacy performance of e-commerce businesses is to use a benchmarking framework that evaluates two dimensions: transparency and control. Transparency refers to how clearly and openly the business communicates its data practices to its customers, such as through privacy policies, notices, and disclosures. Control refers to how much choice and influence the customers have over their data, such as through consent mechanisms, access requests, and deletion options. 15 e-commerce platforms will be selected from the list of top 20 e-commerce sites in Malaysia based on their popularity, market share, and diversity of products and services. The platforms are: Lazada, Shopee, Lelong, Mudah, PrestoMall, Carousell, Ezbuy, Qoo10, PG Mall, YouBeli, Jingdong, Go shop, eBay Malaysia, Eleven Street, and Senheng. The data will be collected from these platforms by reviewing their privacy policies, terms of service, and user interfaces.

The qualitative data sources that were utilized in this inquiry were mostly focused on the core documents and interfaces that define the user experience within e-commerce platforms. This investigation was conducted to gather information. It was primarily through the utilization of privacy policies that we were able to get an understanding of the stated practices of data collection, processing, and sharing. These policies typically contain a significant amount of information regarding legal and procedural matters. The terms of service, which included a description of the contractual arrangements that exist between platforms and users, additionally provided additional context for the situation.

According to the terms conceptual framework and the theoretical framework are frequently and incorrectly understood to be synonymous with one another [32]. The foundation or "lens" through which a study is formed is referred to as a theoretical framework. This framework is responsible for providing the theoretical assumptions that are used in the larger context of a study. The research focus investigation is able to be rooted in theoretical underpinnings with the assistance of this framework, which also helps to frame the inquiry for data analysis and interpretation. The purpose of applying theory in conventional theoretical research is to comprehend, explain, and forecast the occurrence of events [33].

The decision-making process of consumers in the context of e-commerce and data privacy issues is a complex and dynamic behavior shaped by a myriad of factors. As technology advances and digital interactions become integral to everyday life, consumers find themselves navigating a constantly evolving landscape where concerns about data privacy play a significant role in shaping their decisions. The key aspect of the dynamic nature of consumer decision-making in e-commerce is the increasing awareness and sensitivity to data privacy. Consumers are becoming more informed about the ways their personal information is collected, stored, and utilized by online platforms. News of data breaches, cyber-attacks, and privacy scandals has heightened consumer awareness, making them more cautious and discerning in their interactions with e-commerce platforms.

E-ISSN: 2988-3512



Figures 2. Theoretical Framework

Control and Transparency as Independent Variables (IV)

It is of the utmost importance to have a thorough understanding of the intricacies of transparency and control when it comes to the privacy of digital data in the context of online shopping. These components, which serve as Independent Variables (IVs), play a significant role in defining how customers perceive e-commerce platforms, how they behave, and ultimately how successfully the platforms perform from a business perspective. Within the framework of the Communication Privacy Management (CPM) theory, this section investigates the nuances of Transparency, with a particular focus on the Private Information Boundary, and Control, with an investigation into the Private Information Control.

Private Information Boundary

The Private Information Boundary is an essential concept that serves to define the limits of an individual's ability to share personal information and is at the core of the concept of transparency. In essence, it determines the limits of what individuals are willing to divulge for online communication. According to the conceptual definition, the Private Information Boundary is the line that divides personal information from public information. This line indicates the extent to which individuals feel comfortable exposing particular information about themselves.

Control of Private Information

The control of private information is an additional essential component of openness that goes beyond the lines. The sense of control and agency that individuals have over the personal information that they provide is being captured by it. When seen from a conceptual angle, the term "Private Information Control" refers to the degree to which individuals believe they can control and limit the manner in which their data is shared online [34].

Private Information Rules

The cornerstone of control is the formulation and implementation of Private Information Rules, which are a set of guidelines and regulations that individuals devise in order to exercise control over who can access, use, and share their personal information regarding them. With the assistance of these rules, users are able to actively set and enforce the boundaries of their digital privacy.

E-ISSN: 2988-3512

Private Information Co-ownership

The notion of Private Information Co-ownership recognizes the collaborative aspect of privacy management, surpassing individual control. Captures the notion that, depending on the situation, people could jointly be accountable for or own particular bits of personal data. Co-ownership is an indication of mutual understanding and consent between parties about how to handle and access certain data pieces.

Private Information Boundary Turbulence

Limitations on Private Information Turbulence adds a dynamic component to Control by acknowledging that people's boundaries for their private information are susceptible to change and outside factors. It recognises the dynamic nature of privacy management, where people might run into difficulties and doubts while trying to keep their borders around their information stable.

Business Performance (Dependent variable)

Within the framework of e-commerce research, the dependent variable (DV) that is being investigated is the concept of business performance. There are a variety of components that make up this intricate idea, such as the overall competitiveness of the market, the satisfaction of the customers, and the financial results. When seen from a conceptual aspect, business performance refers to the capacity of an e-commerce platform to successfully navigate the digital marketplace by achieving both its operational and strategic objectives.

H_1: Private information boundaries positively enhance the transparency of data privacy policy practices and the business performance of e-commerce companies in Malaysia

H_2: Private Information Control positively enhances the transparency of data privacy policy practices and the business performance of e-commerce companies in Malaysia.

H_3: Private information rules positively enhance the Control of data privacy policy practices of e-commerce companies in Malaysia.

H_4: Private information co-ownership positively enhances the Control of data privacy policy practices of e-commerce companies in Malaysia.

H_5: Private information boundary turbulence negatively impacts the Control of data privacy policy practices of e-commerce companies in Malaysia.

RESULTS AND DISCUSSION

Examination of Qualitative Data

On the basis of the qualitative data that will be acquired, a comprehensive analysis was carried out with the assistance of the NVivo program. With NVivo's assistance, the process of systematically categorizing, organizing, and identifying topics was simplified and made more straightforward. The process of coding involved the categorization of both textual and visual information into themes. This allowed for the identification of recurring patterns and the identification of evolving concepts. It was guaranteed that the analytical process was both methodical and open to scrutiny thanks to this program, which provided a powerful platform for managing the complexity of qualitative data.

Multiple probability and non-probability sampling approaches are available for doing research. The research uses the non-probability convenience sampling approach for sampling. Convenient sampling methodology involves gathering data based on the opportunities, accessibility, and availability of potential participants. The non-probability convenient sampling approach is chosen because it is a cost-effective and practical way to research the hypothesis with few hassles, as the participants are readily accessible [35].

E-ISSN: 2988-3512

The participants in a non-probability convenience sampling method ensurethat the data collected from the respondents are reliable, as the selection criteria would limit the respondents to those who are relevant to the study and, as such, would be more willing to participate in this study [36].

The target population of this study is online shoppers in Malaysia. The population of Malaysia stood at 32.7 million in 2022 (DOSM 2022). According to the Multimedia Commission Report on Internet User Survey (2022), 66% of internet users, i.e., approximately 21.5 million in Malaysia, engage in online shopping. Using Krejcie and Morgan(1970), the sample size for the study is 379. The sample frame for this study is stratified random sampling, which is aimed at representativeness [37].

Online survey questionnaires will be used as the primary data collection method in this study [38]. A survey is a research technique that uses a standardized questionnaire to collect information about attitudes, opinions, behaviors, and backgrounds and lifestyle characteristics from a sample of respondents.

To hasten the process of data collection, the researcher enlisted the help of friends in Selangor, Melaka, Johor, and Penang who were online shoppers, who, in turn, introduced their friends for the administration of the survey. 500 questionnaires were disseminated through these contacts.

Data will be analyzed using the Statistical Package for Social Sciences (SPSS). The analysis included descriptive and inferential statistical analysis. The descriptive statistics included frequency, percentages, means, and standard deviation, while the inferential statistics included a reliability test and correlation [39].

Before administering the survey, a pretest was conducted with the 22 completed questionnaires received via email from the Malaysian journalists to ensure that the questionnaire was adequately designed and contained no errors. The study took internal validity, external validity, and content validity into consideration. The variables were also tested for reliability to determine Cronbach's alpha.

Table 1. Reliability Index of the Variables

No	Alpha	*N* items		
1	.92	42		

The data required for the support and validating qualitative results is unfolded by a .975 value of Cronbach's alpha, which is showing excellent reliability of data fit for analysis of the impact of digital data privacy & Cybersecurity policy on business performance of the E-Commerce Industry in Malaysia, while exploring the role of Transparency & Control.

The results indicate that the instruments were valid, and internal consistency has been confirmed for the dimensions with the application of Cronbach's alpha to examine the internal reliability of the items. Through the execution of a pilot study, the process of validation moves beyond the realm of theoretical alignments and expert assessments and into the realm of actual application. During this stage, the questionnaire will be administered to a small sample that is typical of the demographic that is being targeted. The purpose of this evaluation is to determine how effectively the questionnaire functions in a real-world setting, with the intention of capturing actual replies and subtleties that may not have been obvious during the phases of creation and content validity [40].

The pilot testing phase of the validation process is not only a formality; rather, it is a strategic stage in the process. The purpose of this is to uncover any problems, ambiguities, or misinterpretations that may have been missed by the expert evaluations. Due to the fact that the pilot research is conducted on a smaller scale, it is possible to conduct an in-depth

E-ISSN: 2988-3512

investigation into the manner in which participants interact with the questionnaire. This provides valuable insights that contribute to the iterative development of the instrument [41].

The early analysis of the data collected from the pilot research is performed not to arrive at conclusive results, but rather to shed light on any trends or anomalies in the replies of the participants. For the purpose of providing insights into how well the questionnaire works in terms of clarity, relevance, and efficacy, this preliminary analysis acts as a diagnostic tool. In order to guide additional adjustments, the feedback loop that was begun by the pilot research is utilized. Adjustments are performed to improve the instrument's clarity and sensitivity in the event that particular questions repeatedly evoke misunderstanding or if unanticipated patterns develop. Through this process of iterative refining, the questionnaire will be transformed into a dynamic and resilient instrument that is capable of eliciting responses that are both accurate and meaningful by the time the validation procedure is complete [41].

The rapid expansion of the e-commerce industry has transformed business models, consumer behavior, and value creation in the digital economy. However, this growth is inseparable from increasing concerns over data privacy and cybersecurity, which directly affect consumer trust and, ultimately, business performance. This study critically analyzes how transparency and control within data privacy policies shape the performance of e-commerce firms, particularly in the Malaysian context, where digital commerce is growing rapidly and contributes significantly to national income. A central argument of the research is that data privacy is no longer a purely legal or technical issue but a strategic business resource. E-commerce platforms collect vast amounts of consumer data to personalize services, optimize operations, and enhance competitiveness. While such practices can improve efficiency and profitability, they simultaneously raise consumer anxieties regarding surveillance, misuse of personal information, and data breaches. The study demonstrates that when these concerns are not adequately addressed, they erode trust and negatively influence purchasing decisions, platform loyalty, and long-term performance [42].

Analysis

The analysis is grounded in Communication Privacy Management (CPM) theory and Behavioral Decision Theory (BDT), which together provide a robust explanatory framework. CPM theory highlights how consumers perceive ownership, boundaries, and control over their personal information. Transparency in privacy policies clarifies these boundaries, enabling users to understand what data are collected, how they are used, and with whom they are shared. Control mechanisms—such as consent options, data access, modification, and deletion—empower users and reinforce their sense of agency. The study finds that platforms with clearly articulated privacy boundaries and strong control mechanisms tend to generate higher levels of consumer trust, which positively correlates with business performance indicators. Behavioral Decision Theory further explains how transparency and control influence consumer choices. In digital environments characterized by uncertainty and risk, consumers rely heavily on perceived trustworthiness when making decisions. Transparent data practices reduce perceived risk, while control mechanisms increase perceived benefits by allowing users to manage their data proactively. The analysis suggests that consumers are more willing to share data and engage in transactions when they believe the platform respects their privacy rights, creating a virtuous cycle between trust, data sharing, and performance [42].

The study’s mixed-methods approach strengthens its analytical depth. Qualitative benchmarking reveals disparities among Malaysian e-commerce platforms, with major players such as Lazada and Shopee exhibiting higher levels of transparency and control compared to smaller platforms. Quantitative findings from 379 respondents further confirm that transparency and control significantly enhance business performance, while privacy boundary turbulence negatively affects perceived control. Overall, this analysis underscores that effective data privacy governance is a critical driver of cybersecurity, consumer trust, and sustainable business performance. By integrating transparency and control into privacy

E-ISSN: 2988-3512

policies, e-commerce firms can transform privacy compliance from a regulatory obligation into a strategic advantage within the competitive digital marketplace [43].

CONCLUSION

This study investigates the impact of digital data privacy policies on the business performance of e-commerce companies in Malaysia, with a focus on the mediating roles of transparency and control. As data privacy concerns escalate in the digital age, understanding how e-commerce platforms manage user data is critical for sustaining trust and competitiveness. The research employs a mixed-methods approach, combining qualitative benchmarking of data privacy policies from major e-commerce platforms (e.g., Lazada, Shopee, Carousell) with quantitative surveys of 379 online shoppers. Key findings indicate that higher levels of transparency and control in data privacy practices are associated with improved business performance. Specifically, clear private information boundaries and robust control mechanisms enhance user trust, while factors like boundary turbulence negatively impact perceived control. The study underscores the importance of aligning data privacy policies with user expectations to foster trust and loyalty in Malaysia's growing e-commerce sector. It recommends that e-commerce platforms prioritize transparent communication of data usage and empower users with control options. Policymakers can leverage these insights to strengthen data protection regulations, promoting a secure digital economy. Future research could explore cross-industry comparisons or assess the impact of emerging technologies on privacy dynamics. This study serves as a foundation for balancing business interests with user privacy rights in Malaysia's digital landscape. The process of validation as it transitions from qualitative to quantitative is a painstaking journey that encompasses expert reviews, content validity assessments, and pilot testing in the real world. To ensure that the questionnaire accurately reflects the intricate relationship that exists between digital data privacy, user perceptions, and company success in the context of Malaysia's e-commerce ecosystem, it is not a linear development but rather an iterative cooperation between researchers and subject matter experts. The incorporation of qualitative insights into the validation process is more than just a simple checkbox; it guarantees that the subtleties that are discovered via qualitative means are not lost but are correctly reflected in the quantitative investigation. As we move forward, we are prepared to collect data that not only quantifies but also fully understands the complexities of user experiences and expectations in the ever-evolving area of digital data protection. This is because we are armed with a verified questionnaire.

Acknowledgments

The authors express sincere gratitude to the Faculty of Business Technology, University of Cyberjaya, Malaysia, and partner institutions in Pakistan for academic support, data access, and constructive discussions that enriched this study on data privacy, cybersecurity, and business performance in the e-commerce industry.

Author's Contributions

All authors contributed collaboratively to this research. Conceptualization and design were developed jointly. Data analysis and interpretation were conducted collectively. Drafting and critical revision of the manuscript were shared equally, ensuring intellectual rigor, coherence, and relevance to data privacy, transparency, and cybersecurity in e-commerce.

Conflicts of Interest

The authors declare no conflicts of interest related to this study. The research was conducted independently without financial, institutional, or commercial influences that could bias the analysis, interpretation, or conclusions regarding data privacy, cybersecurity transparency, control mechanisms, and business performance in the e-commerce industry.

E-ISSN: 2988-3512

REFERENCES

[1] E. Buçaj and K. Idrizaj, "The need for cybercrime regulation on a global scale by the international law and cyber convention," *Multidiscip. Rev.*, vol. 8, no. 1, pp. 2025024–2025024, 2025, https://doi.org/10.31893/multirev.2025024.

[2] A. R. Hidayat, "Leveraging Artificial Intelligence for Real-Time Production Optimization in Smart Manufacturing Systems," *J. Prod. Manag. Optim.*, vol. 1, no. 1, pp. 34–42, 2025, [Online]. Available: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Qudus%2C+2025&btnG=

[3] T. M. Choi, S. Kumar, X. Yue, and H. L. Chan, "Disruptive Technologies and Operations Management in the Industry 4.0 Era and Beyond," *Prod. Oper. Manag.*, vol. 31, no. 1, pp. 9–31, 2022, https://doi.org/10.1111/poms.13622.

[4] H. Guo *et al.*, "A highly sensitive, self-powered triboelectric auditory sensor for social robotics and hearing AIDS," *Sci. Robot.*, vol. 3, no. 20, p. 2516, 2018, https://doi.org/10.1126/SCIROBOTICS.AAT2516.

[5] Y. Malakar, L. J. M. Peeters, A. Walton, and D. O'Sullivan, "A causal network approach using a community well-being framework for an initial impact assessment of large-scale energy infrastructure projects," *Environ. Impact Assess. Rev.*, vol. 102, p. 107188, 2023, https://doi.org/10.1016/j.eiar.2023.107188.

[6] V. Bentotahewa, C. Hewage, and J. Williams, "Solutions to Big Data Privacy and Security Challenges Associated With COVID-19 Surveillance Systems," *Front. Big Data*, vol. 4, p. 645204, 2021, https://doi.org/10.3389/fdata.2021.645204.

[7] H. Habib *et al.*, "Away from prying eyes: Analyzing usage and understanding of private browsing," in *Proceedings of the 14th Symposium on Usable Privacy and Security, SOUPS 2018*, 2018, pp. 159–175. [Online]. Available: https://www.usenix.org/conference/soups2018/presentation/habib-prying

[8] L. J. Bowman, "Statista," *J. Bus. Financ. Librarianship*, vol. 27, no. 4, pp. 304–309, 2022, https://doi.org/10.1080/08963568.2022.2087018.

[9] M. Kangwa, C. S. Lubobya, and J. Phiri, "Protection of personally identifiable Information and Privacy via the use of Hardware and Software," *Lect. Notes Eng. Comput. Sci.*, vol. 2243, no, pp. 75–81, 2021.

[10] O. N. Whitney *et al.*, "Sewage, Salt, Silica, and SARS-CoV-2 (4S): An Economical Kit-Free Method for Direct Capture of SARS-CoV-2 RNA from Wastewater," *Environ. Sci. Technol.*, vol. 55, no. 8, pp. 4880–4888, 2021, https://doi.org/10.1021/acs.est.0c08129.

[11] M. J. Metzger, "Making sense of credibility on the web: Models for evaluating online information and recommendations for future research," *J. Am. Soc. Inf. Sci. Technol.*, vol. 58, no. 13, pp. 2078–2091, 2007, https://doi.org/10.1002/asi.20672.

[12] A. F. Westin, "Special report: Legal safeguards to ensure privacy in a computer society," *Commun. ACM*, vol. 10, no. 9, pp. 533–537, 1967, https://doi.org/10.1145/363566.363579.

[13] S. Petronio, "Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation?" *J. Fam. Theory Rev.*, vol. 2, no. 3, pp. 175–196, 2010, https://doi.org/10.1111/j.1756-2589.2010.00052.x.

[14] V. Varlina, D. W. Junaidy, L. Mawali, Y. A. Piliang, and A. Matsumae, "Effects of decreased visual–auditory multisensory stimuli on creativity: a conceptual network analysis," *Des. Sci.*, vol. 11, p. 42, 2025, https://doi.org/10.1017/dsj.2025.10035.

[15] G. D. Traviss-Turner, R. M. West, and A. J. Hill, "Guided Self-help for Eating Disorders: A Systematic Review and Metaregression," *Eur. Eat. Disord. Rev.*, vol. 25, no. 3, pp. 148–164, 2017, https://doi.org/10.1002/erv.2507.

[16] S. W. Littlejohn and K. A. Foss, "Theories of Human Communication," vol. 10: 25. Query date, p. 36, 2008. [Online]. Available: http://books.google.com/books?hl=id&lr=&id=r3Fk0aRpJM4C&pgis=1

[17] L. T. Lee, "Privacy and social media," *The Social Media Industries*. pp. 146–165, 2013. https://doi.org/10.4324/9780203121054.

[18] S. Petronio and J. Reierson, "Regulating the privacy of confidentiality: Grasping the complexities through communication privacy management theory," in *Uncertainty, Information Management, and Disclosure Decisions: Theories and Applications*, 2015, pp. 365–383. https://www.taylorfrancis.com/chapters/edit/10.4324/9780203933046-25/regulating-privacy-confidentiality-sandra-petronio-jennifer-reierson

[19] W. Chiu and H. Cho, "E-commerce brand: The effect of perceived brand leadership on consumers' satisfaction and repurchase intention on e-commerce websites," *Asia Pacific J. Mark. Logist.*, vol. 33, no. 6, pp. 1339–1362, 2019, https://doi.org/10.1108/APJML-10-2018-0403.

E-ISSN: 2988-3512

[20] C. Jane Hollowell, Z. Rowland, T. Kliestik, J. Kliestikova, and V. V. Dengov, "Customer loyalty in the sharing economy platforms: How digital personal reputation and feedback systems facilitate interaction and trust between strangers," *J. Self-Governance Manag. Econ.*, vol. 7, no. 1, pp. 13–18, 2019, https://doi.org/10.22381/JSME7120192.

[21] R. Tuyls and A. Pera, "Innovative data-driven smart urban ecosystems: Environmental sustainability, governance networks, and the cognitive internet of things," *Geopolit. Hist. Int. Relations*, vol. 11, no. 1, pp. 116–121, 2019, https://doi.org/10.22381/GHIR11120198.

[22] L. R. Waitman *et al.*, "Enhancing PCORnet Clinical Research Network data completeness by integrating multistate insurance claims with electronic health records in a cloud environment aligned with CMS security and privacy requirements," *J. Am. Med. Informatics Assoc.*, vol. 29, no. 4, pp. 660–670, 2022, https://doi.org/10.1093/jamia/ocab269.

[23] K. L. Brown-Jackson, "Grasping Cybersecurity Leadership as It Relates to Critical Infrastructure Protection," *Int. J. Smart Educ. Urban Soc.*, vol. 13, no. 1, pp. 1–14, 2022, https://doi.org/10.4018/ijseus.312233.

[24] K. Ristovska and C. M. Bande, "Machine learning vs. data mining: Understanding the differences and intersections," *Int. J. Sci. Res. Publ.*, vol. 15, no. 1, pp. 130–136, 2025, https://doi.org/10.29322/ijsrp.15.01.2025.p15718.

[25] DIGITAL ART, "The Evolution and Impact of Pop Art in the Digital Age," *Home Art Haven*, vol. 7, no. 5, pp. 834–839, [Online]. Available: https://homearthaven.com/blogs/news/the-evolution-and-impact-of-pop-art-in-the-digital-age

[26] I. Susilowati, "Legal Perspectives on Data Privacy and Cybersecurity in the Digital Age," *Int. J. Soc. Rev.*, vol. 3, no. 2, pp. 471–481, 2025, [Online]. Available: https://www.researchgate.net/profile/Muh-Fauzan-Nastiar/publication/389499994_LEGAL_PERSPECTIVES_ON_DATA_PRIVACY_AND_CYBERSECURITY_IN_THE_DIGITAL_AGE/links/67c4d7ac645ef274a499399f/LEGAL-PERSPECTIVES-ON-DATA-PRIVACY-AND-CYBERSECURITY-IN-THE-DIGITAL-AGE.pdf

[27] T. W. Sanchez, M. Brenman, and X. Ye, "The Ethical Concerns of Artificial Intelligence in Urban Planning," *J. Am. Plan. Assoc.*, vol. 91, no. 2, pp. 294–307, 2025, https://doi.org/10.1080/01944363.2024.2355305.

[28] R. Kipyegon, "Information System Audit Strategies and Data Security Measures Among Commercial Banks in Kenya." 2023. [Online]. Available: https://erepository.uonbi.ac.ke/handle/11295/167645

[29] E. F. Zineb, R. Najat, and A. Jaafar, "An Intelligent Approach for Data Analysis and Decision Making in Big Data: A Case Study on E-commerce Industry," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 7, pp. 723–736, 2021, https://doi.org/10.14569/IJACSA.2021.0120783.

[30] M. Borgstede and M. Scholz, "Quantitative and Qualitative Approaches to Generalization and Replication–A Representationalist View," *Front. Psychol.*, vol. 12, p. 605191, 2021, https://doi.org/10.3389/fpsyg.2021.605191.

[31] Creswell J, "Revisiting mixed methods and advancing scientific practices," *The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry*. pp. 61–71, 2015. https://doi.org/10.1093/oxfordhb/9780199933624.013.39

[32] C. Grant and A. Osanloo, "Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for Your 'House,'" *Adm. Issues J. Educ. Pract. Res.*, vol. 4, no. 2, p. 4, 2014, https://doi.org/10.5929/2014.4.2.9.

[33] R. A. Swanson and T. J. Chermack, *Theory Building in Applied Disciplines*, vol. 5, no. 1. Berrett-Koehler Publishers, 2014. https://doi.org/10.1108/jchrm-06-2013-0023.

[34] H. Kang, "Sample size determination and power analysis using the G*Power software," *J. Educ. Eval. Health Prof.*, vol. 18, 2021, https://doi.org/10.3352/JEEHP.2021.18.17.

[35] H. Taherdoost, "Sampling Methods in Research Methodology: How to Choose a Sampling Technique for Research," *SSRN Electron. J.*, 2018, https://doi.org/10.2139/ssrn.3205035.

[36] I. Etikan, "Comparison of Convenience Sampling and Purposive Sampling," *Am. J. Theor. Appl. Stat.*, vol. 5, no. 1, p. 1, 2016, https://doi.org/10.11648/j.ajtas.20160501.11.

[37] H. S. Nawwal, "Magnetic Nanostructures." American Scientific Publishers, Los Angeles, 2023.

[38] M. E. McCombs and P. M. Poindexter, "Research in mass communication: A practical guide." p. 451, 1999. [Online]. Available: https://cir.nii.ac.jp/crid/1971149384865081871

[39] Muthoifin and P. Putri, "Social Level Parameters of Banjar Society in the Tradition of Jujuran Islamic Law Perspective," *Proc. Int. Conf. Eng. Technol. Soc. Sci. (ICONETOS 2020)*, vol. 529, no. Iconetos 2020, pp. 87–90, 2021, https://doi.org/10.2991/assehr.k.210421.014.

[40] R. Crawford, "Information technology in secondary schools and its impact on training information technology teachers," *J. Inf. Technol. Teach. Educ.*, vol. 9, no. 2, pp. 183–198, 2000, https://doi.org/10.1080/14759390000200082.

[41] A. MacPhail, M. Ulvik, A. Guberman, G. Czerniawski, H. Oolbekkink-Marchand, and Y. Bain, "The professional development of higher education-based teacher educators: needs and realities," *Prof. Dev. Educ.*, vol. 45, no. 5, pp. 848–861, 2019, https://doi.org/10.1080/19415257.2018.1529610.

[42] T. Van Waeyenberg, R. Peccei, and A. Decramer, "Performance management and teacher performance: the role of affective organizational commitment and exhaustion," *Int. J. Hum. Resour. Manag.*, vol. 33, no. 4, pp. 623–646, 2022, https://doi.org/10.1080/09585192.2020.1754881.

[43] H. V Jansen, N. R. Tas, and J. W. Berenschot, "Encyclopedia of nanoscience and society," *Choice Reviews Online*, vol. 48, no. 07. American Scientific Publishers, Los Angeles, pp. 48-3608-48–3608, 2011. https://doi.org/10.5860/choice.48-3608.

E-ISSN: 2988-3512