Labuan Bulletin of International Business &Finance

Volume 22 Issue 1 eISSN 2600- 7894

PRIVACY CONCERNS AND CONSUMERS' TRUST IN M-COMMERCE APPS IN MALAYSIA

Nur Hikmah Masran[a] & Azaze-Azizi Abdul Adis[a*]

[a]Faculty of Business, Economics and Accountancy
Universiti Malaysia Sabah
**Corresponding author: azizi@ums.edu.my*

ABSTRACT

Apps for mobile devices have become crucial in daily life. Every day, millions of people rely on smartphone apps to perform a variety of crucial tasks. Mobile app shops have seen an expansion in the number of apps due to rising consumer demand. On the other hand, as people's concerns about online privacy have grown, privacy issues pertaining to internet use have become more important in recent years. However, this study found that building trust might help allay consumers' worries about privacy when it comes to using m-commerce apps in Malaysia. Consequently, the purpose of this study is to empirically investigate customers' trust by comprehending privacy concerns related to their use of m-commerce apps in Malaysia. The APCO model and Social Cognitive Theory (SCT) are further explored in this study. Data were gathered through an online survey conducted on Malaysian users of mobile applications. Only 292 of the 350 respondents' useful responses were examined using SPSS and SmartPLS statistical tools. The results demonstrated and validated (APCO) and (SCT) emphasis on people examining the risks and benefit when deciding whether to disclose personal information. Practitioners would apply the empirical findings to study and comprehend consumer preferences in light of these results.

JEL classification*: M3*
Keywords*: Privacy Concerns; Trust, M-Commerce Apps; APCO; SCT and Malaysia*

Received: March 18, 2024
Revised: August 9, 2024
Accepted: September 10, 2024

1. INTRODUCTION

Rocha et al. (2020) claim that there has been a significant increase in the number and usage of mobile applications in recent years, which has altered how customers go about their everyday lives and do business. Everyday tasks like making phone calls, paying bills, and shopping online can all be done with apps (Rocha et al., 2020). Mobile apps are becoming integrated and commonplace in consumers' daily lives due to the quick development of mobile communication technology (Kang & Namkung, 2019). This led to the emergence of m-commerce, which is characterized as an extension of e-commerce

in which commercial transactions are conducted in a wireless setting using mobile devices. Moreover, it has transformed the e-commerce user experience and created a new avenue for businesses to provide customers with more focused and specialized offers (Chopdar et al., 2018).

Consumers' concerns about privacy have endured for a long time, despite the advantages of technology advancement. In today's globalized world, the need for privacy has been widely and unequivocally argued (Foltz & Foltz, 2020). Thanks to advancements in technology, most companies can now gather and handle personal data on a never-before-seen scale. In the digital age, data collection and processing have elevated privacy to the top of the list of moral, social, and legal concerns. Online personal data gathering, use, and sharing can restrict an individual's identity and enable consumer identity theft, phishing, tracking, manipulation, and discrimination, among other abuses (Anic et al., 2019). Because digital services like mobile applications have such a high demand for user data, consumer privacy is put even more at risk (Kang & Namkung, 2019).

This study's objective is to examine the relationship between app permission concerns, privacy awareness, privacy experience, and self-efficacy on privacy concerns. This study also examines how privacy issues impact consumer perceptions of trust towards m-commerce app usage in Malaysia. In the context of an m-commerce app, such as "Foodpanda, Lazada, Shopee, etc," privacy concerns significantly impact user trust. The app collects a range of data, including location data for personalized offers, browsing history for product recommendations, and payment information for transactions (Betzing et al., 2019). Users often express apprehension about the extent of data collection and its potential misuse. Specifically, they worry about the scope of data collected, including whether their location and browsing history are used beyond what they expected, and whether their data might be shared with third parties or compromised through security breaches (Hudson & Liu, 2021; Zhou, 2020). These privacy concerns can lead to a decrease in trust, affecting users' willingness to engage with the app and make purchases. To address these issues, research can focus on how these concerns influence user trust, evaluating the effectiveness of privacy practices such as transparent data policies, strong security measures, and user control options (Bhattacharya et al., 2022). Understanding how these factors affect trust can help identify strategies to enhance user confidence and improve their overall experience with the m-commerce app.

This study would make significant theoretical contributions by validating the roles of app permission concerns, privacy awareness, privacy experience, and self-efficacy as key factors influencing user trust in m-commerce apps through privacy concerns. Traditional theories of trust often focus on general factors affecting trust but may not fully address how specific privacy-related variables interact to influence trust. By demonstrating that all proposed variables would be significant and supported, this study enhances existing theoretical models by providing empirical evidence of their importance.

These insights challenge and refine traditional trust theories by illustrating that user trust is not merely influenced by overarching privacy issues but is significantly impacted by several specific aspects such as privacy management and user perceptions (Koohikamali et al., 2019; Li et al., 2019). This study highlights the complexity of privacy concerns as a mediator and underscores the need for trust theories to incorporate detailed privacy variables. Additionally, by validating the significance of these variables, this study provides a more robust theoretical framework that enhances understanding of how privacy concerns and trust interact. This contribution is particularly valuable for

designing more effective privacy strategies in m-commerce apps, as it provides a detailed model of how various privacy factors collectively influence user trust. Furthermore, the findings set a foundation for future research to explore how these relationships may evolve with emerging privacy technologies, offering a pathway for further theoretical development in the field.

2. LITERATURE REVIEW

2.1 Literature Gap

While existing research extensively examines the impact of privacy concerns on trust in various online environments, there is a notable gap in studies focusing specifically on m-commerce apps, particularly in regional contexts like Malaysia. Previous research by Wottrich et al. (2018); Dogruel et al. (2023); and Cloarec (2022), have investigated privacy concerns broadly but often overlooks the distinct privacy issues associated with app permissions, privacy awareness, privacy experience, and self-efficacy within m-commerce platforms. Furthermore, the interaction between these variables in influencing trust through privacy concerns has not been thoroughly explored in this context. This study addresses these gaps by providing new insights into how specific privacy concerns, app permissions concerns, privacy awareness, privacy experience, and self-efficacy affect trust in m-commerce apps. By analyzing data from a focused sample of Malaysian consumers, the study offers a region-specific perspective that enriches the understanding of these dynamics.

Additionally, it extends the APCO model, privacy calculus theory, and social cognitive theory by integrating the role of app permission concerns, privacy awareness, privacy experience, and self-efficacy toward privacy concerns and trust in a novel way. The findings also have practical implications for m-commerce platforms, offering actionable recommendations for improving privacy practices to enhance consumer trust. This approach not only extends theoretical frameworks but also introduces innovative methodological aspects, contributing significantly to both academic research and practical applications in the field of m-commerce among Malaysian consumers.

2.2 Mobile Perception

Location data is often disclosed by mobile apps, and this is sometimes coupled with demands for additional types of private information (Keith et al., 2013). Because of this, users' privacy worries outweigh many apps' values when using them (Keith, Lowry, et al., 2016). The ability of an individual to control when, how, and how much of their personal data is shared with mobile applications is how the researchers defined information privacy in the context of apps (Hong & Thong, 2013; Keith et al., 2016).

Consumer privacy concerns are a major factor in the data collection and management procedures that businesses use to handle shared data (Balapour et al., 2020). Based on recent studies (Alzaidi et al., 2022; Tay et al., 2021; Koohikamali et al., 2019) privacy concerns can be seen as a multifaceted construct that includes understanding of current privacy policies, information management by the party to which the user provides personal data, and management of interactions between the user and third parties. Furthermore, a person's views about privacy have an impact on their attitudes and behaviors, including trust. Consumers who want more information transparency are less willing to disclose personal information, according to the privacy paradox (Balapour et al., 2020).

In the era of m-business, consumers are drawn to a variety of functions and applications on mobile devices, such as entertainment and location-based services. Customers are frequently asked for pertinent information, including location and payment details, to enjoy mobile app features or to buy rewards like points and coupons (Wang et al., 2016). When an enormous quantity of highly detailed personal data is made public, there is a greater possibility of it being compromised or misused. The paradox of receiving personalized services and running the risk of losing personal information is evident in m-business. When faced with a situation like this, an online company needs to figure out how to convince customers that the advantages outweigh the possible expenses of data misuse by the supplier and its connected companies. A substantial amount of research has been done on information privacy in both the digital and physical realms. On the other side, consumers worry about their personal data being illegally collected, stored, profiled, and used for illegal purposes (Wang et al., 2016).

2.3 App Permission Concerns and Privacy Concerns

App permissions are defined as requests made by applications to access specific operations or core functionalities of a device. These permissions can include sensitive information such as phone numbers, address books, precise locations, and SMS messages, making privacy a significant concern in the Android permission model (Olukoya et al., 2020). The app permission model governs how applications access sensitive resources, including personal information and sensor data like cameras and GPS (Bhandari et al., 2017). As noted by Bhandari et al. (2017), app permissions also positively influence individuals' privacy concerns. For example, users may be particularly attentive to permissions such as “READ_CONTACTS,” which can highlight the security or privacy implications associated with an app’s use. This study refers to app permission concerns as requests made by applications to access specific operations or core functionalities of a device when using m-commerce platforms.

Hence, this study believed a positive relationship existed between app permission and privacy concerns. As supported by Degirmenci (2020), growing concerns about app permission requests can heighten consumers' overall discomfort regarding privacy. This study specifically examines app permission requests related to the increasing collection of personal data through m-commerce apps, which can lead to excessive data collection and heightened information privacy concerns. Mobile consumers are less likely to accept app permission requests that exceed the app's necessary functions due to privacy concerns about potentially exposed personal data (Degirmenci, 2020). Similar work also by Polykalas and Prezerakos (2019) supported the relationship between app permission concerns and privacy concerns. Permissions required by an app are classified as dangerous if they have the potential to harm the user or their device. For example, dangerous permissions may allow an application to access personal information such as contacts and addresses, which can pose significant privacy risks (Polykalas & Prezerakos, 2019).

Nonetheless, when accepting permission, in this study context, the consumers would consider the apps’ features to enhance their perception of the actual behavior of Android applications and the detection of malicious apps (Olukoya et al., 2020). It is important for consumers to be aware of app permission requests before downloading an app, as this allows them to evaluate potential privacy risks beforehand. Consequently, heightened concern about app permissions tends to amplify consumers' privacy concerns (Wang et al., 2020). Therefore, it is hypothesized that:

H1: App permission concern has a positive effect on privacy concerns.

2.4 Privacy Awareness and Privacy Concerns

Privacy awareness refers to the extent of an individual's knowledge about general information privacy practices and their application in mobile apps (Smith et al., 2011; Malhotra et al., 2004). This awareness can have an effect on a person's attitudes and perceptions towards m-commerce apps (Balapour et al., 2020). This study refers to privacy awareness as consumers' knowledge about general information privacy practices when using m-commerce platforms.

Individuals with high privacy awareness are particularly cautious when disclosing their data for subsequent use. This awareness does not deter them from self-disclosure but rather informs their decisions about privacy. Research by Belanger et al. (2019) indicates that higher privacy awareness typically leads to increased privacy concerns. Consumers who are aware of potential privacy breaches can make informed decisions, adjust their privacy settings, and exercise caution when revealing personal data while using mobile apps. This proactive approach helps mitigate the risk of privacy violations. As also supported by Soumelidou and Tsohou (2020), consumers make informed decisions due to their awareness of potential privacy breaches that could cause harm and increase privacy concerns when using mobile apps. In other words, knowing about possible privacy violations can alert individuals, prompting them to adjust their privacy settings. Consequently, they are likely to be more cautious about sharing personal information.

Moreover, according to Wang et al. (2019), different levels of privacy awareness indicate how well a person grasps the impact of these factors on their ability to safeguard their privacy. As a result, higher privacy awareness can predict greater privacy concerns, as individuals who are more aware are more likely to scrutinize and address privacy issues, including relevant practices and policies (Warner & Wang, 2019). Furthermore, Skrinjaric et al. (2018) concluded that individuals who are more familiar with the privacy policies in place are better equipped to identify potential system vulnerabilities, thereby improving their online privacy. Hence, this study believed that consumers would be aware of any potential breaches when using m-commerce app(s). Thus, it is hypothesized that:

H2: Privacy awareness has a positive effect on privacy concerns.

2.5 Privacy Experience and Privacy Concerns

Privacy experience refers to individuals who have been exposed to or have fallen victim to personal information abuse, leading to heightened concerns about information privacy (Smith et al., 2011). Individuals with previous experiences with compromised information are more likely to be more concerned about information disclosure (Belanger et al., 2019). This study refers to privacy experience as the consumers who have been exposed to or have fallen victim to personal information abuse, leading to heightened concerns about information privacy when using m-commerce app platforms.

A study by Li et al. (2019), also supports the positive relationship between privacy experience and privacy concerns. Individuals tend to rely more on their direct experiences to predict future outcomes because these experiences make knowledge more readily accessible and reduce the chances of missing important events. As a result, past negative experiences can improve individuals' ability to assess risks. Meanwhile, Distler et al. (2020) highlighted that users are highly concerned about past privacy breaches and the

potential misuse of information gathered from the internet. In such cases, users may perceive themselves as victims of personal data misuse (Distler et al., 2020).

Therefore, this demonstrates that consumers with such experiences tend to be more vigilant and cautious to avoid similar issues. Foltz and Foltz (2020) also support this view, showing that individuals who learn from past experiences tend to become more cautious and conservative. Prior privacy experience, which includes previous exposure to privacy breaches, shows that those who have frequently encountered privacy invasions are more concerned about their privacy. As a result, they are less inclined to disclose personal information or use technologies that involve data sharing (Foltz & Foltz, 2020). The more experience consumers have with data breaches, the lower their confidence in handling their data responsibly. This can lead to heightened privacy concerns. Yeh et al. (2019) also support this finding, indicating that in the e-commerce context, experiences of privacy invasion are positively associated with increased information privacy concerns (Yeh et al., 2018).

Another study by Jaspers and Pearsons (2022) also supported the relationship between privacy experience and privacy concerns. Individuals who have experienced personal information misuse through mobile apps tend to be more cautious about their privacy. They may recognize that fraudsters could exploit their data via mobile apps, leading to increased concerns about using smartphones for financial transactions. This heightened apprehension often stems from their past privacy experiences and fear of becoming victims of data theft. This increased worry about privacy is supported by Chatterjee et al. (2022). Additionally, other research has confirmed that past privacy experiences positively influence privacy concerns (Škrinjarić et al., 2018). Thus, it is hypothesized that:

H3: Privacy experience has a positive effect on privacy concerns.

2.6 Self-Efficacy and Privacy Concerns

According to Compeau and Higgins, (1995), self-efficacy can be defined as the belief that a person can perform a particular behavior. Self-efficacy perceptions have also influenced decisions about what behaviors to undertake (Compeau & Higgins, 1995). This study refers to self-efficacy as the capability and confidence that consumers have in using m-commerce app platforms.

Giwah et al. (2020) argue that self-efficacy is relevant in mobile computing, suggesting that individuals with higher self-efficacy in managing their data and information are likely to have fewer privacy concerns. Self-efficacy in technology use has been shown to affect behavior, as individuals with high self-efficacy are more confident in preventing misuse and are motivated to improve their technological knowledge (Akhter, 2014; Butler, 2020). This result is also supported by Belanger et al. (2019) which posited self-efficacy in terms of mobile platform settings and belief in mobile privacy protection. Self-efficacy affects individuals' intentions to protect their mobile information, as they need to feel confident in their ability to correctly configure their device settings. A person's self-efficacy in mobile privacy protection influences their likelihood to plan and implement necessary precautions, which are essential for preventing unintended or unauthorized disclosure of information from their devices (Belanger et al., 2019).

It is also argued that individuals with higher abilities are generally less concerned about their personal information (Chen & Chen, 2015) (Chen & Chen, 2015). Self-

efficacy boosts individuals' confidence in utilizing privacy protection features. With a better understanding of what personal information is collected and how it is used, individuals can reduce their privacy concerns (Cheng et al., 2022). Consequently, this study posits that as consumers gain more online experience in using m-commerce apps, their privacy concerns diminish, leading to a greater willingness to share personal information. Consumers with high levels of privacy self-efficacy are likely to perceive lower risks. Thus, it is hypothesized that:

H4: Self-efficacy has a negative effect on privacy concerns.

2.7 Privacy Concerns and Trust

According to Smith et al. (1996) and Smith et al. (2011), privacy concerns refer to individuals' apprehensions regarding how organizations handle and protect their personal information. This study refers to privacy concerns as consumers' concerns about their information being handled and collected by organizations or app providers. Several studies by Alzaidi and Agag (2022); Ozturk et al., (2017); Zhou (2020), and Walter and Abendroth (2020) supported the negative relationship between privacy concerns and trust. Users who are worried about their information privacy tend to exhibit lower levels of trust towards service providers (Ozturk et al., 2017). Additionally, users with high privacy concerns often question the integrity of service providers in handling their data appropriately in their study context (Walter & Abendroth, 2020). A study by Boo and Chua (2022) also found a negative relationship between privacy concerns and trust.

Similarly, Zhou (2020) found a significant negative relationship between privacy concerns and trust. Users with high privacy concerns may feel they lack control over their personal information and question whether a platform has the capability and integrity to safeguard their privacy, which can lead to a decrease in their trust (Zhou, 2020). Additionally, Slyke et al. (2006) found that individuals who are concerned about the collection, accuracy, and protection of their personal information may be skeptical about a merchant's ability to handle and safeguard their data. Moreover, Alzaidi and Agag (2022) also observed that privacy concerns significantly negatively impact consumers' trust. Therefore, this study hypothesized that:

H5: Privacy concerns have a negative effect on trust.

2.8 Privacy Concerns as a Mediator

According to Smith et al. (1996) and Smith et al. (2011), privacy concerns can be defined as individuals' concerns about organizational practices in managing information privacy. Researchers in the privacy research literature have generally used the construct of privacy concerns to explain privacy behaviors (Smith et al., 2011). The current study posits that privacy concerns are predictors of well-explained individual behavior. The previous studies explained below have thoroughly operationalized privacy concerns in their study contexts (Alzaidi & Agag, 2022; Bawack et al., 2021; Kolotylo-Kulkarni et al., 2021; Tay et al., 2021). Several pioneering privacy studies have attempted to further conceptualize and operationalize privacy concerns in more detail.

Originally, the Concern for Information Privacy (CFIP) scale was developed by Smith et al. (1996), which categorized four data-related dimensions of privacy concerns (collection, errors, secondary use, and unauthorized access to information) that have since served as one of the most reliable instruments measuring individuals' concerns towards

organizational privacy practices (Xu et al., 2008). Generally, Concern for information privacy (CFIP) and a multi-dimensional scale of Internet consumers' information privacy concerns (IUIPC) are two dominant scales to analyze and evaluate privacy concerns. Smith et al. (1996), proposed CFIP, which includes four data-related dimensions of privacy concerns: collection, errors, secondary use, and unauthorized access to information, and established a 15-item instrument (Dinev, 2014; Dinev & Hart, 2004, 2006; Smith et al., 1996, 2011). Meanwhile, IUIPC was developed by Malhotra (Malhotra et al., 2004). The scholars have operationalized a multi-dimensional IUIPC and adapted CFIP into the context of the Internet.

Research has demonstrated how privacy concerns play a mediating role in the relationship between trust and exogenous variables (Smith et al., 2011). Research suggests that privacy concerns act as a mediator between app permission concerns and trust. For instance, individuals who have higher concerns about app permissions tend to have increased privacy concerns. These heightened privacy concerns, in turn, lead to decreased trust in the app or the platform (Bansal et al., 2016). The study also demonstrated that individuals who are more concerned about the permissions requested by location apps tend to have higher privacy concerns. These privacy concerns, in turn, lead to decreased trust in the app's ability to safeguard their location data (Sun et al., 2015). On the other hand, a study by Hudson and Liu (2021) suggests that certain mitigating factors can influence the negative impact of privacy concerns on trust. Providing assurances regarding data protection and security measures can alleviate privacy concerns and enhance trust (Hudson & Liu, 2021).

The relationship between privacy awareness and trust is affected by individuals' level of privacy concerns. As privacy awareness grows, so do concerns about privacy, which in turn influences the degree of trust individuals place in organizations or service providers with their personal information (Chong & Ma, 2021). As individuals become more aware of privacy issues, they are likely to scrutinize more closely how their personal information is managed by organizations and individuals (Correia & Compeau, 2017). Therefore, individuals tend to have less trust in sharing personal information with websites that they perceive as having inadequate privacy practices and insufficient protection for their privacy (Soumelidou & Tsohou, 2020).

This study also posits that privacy concerns mediate the relationship between privacy experience and trust. Individuals who have experienced privacy violations first hand are likely to be more sensitive and vigilant about protecting their personal information. Their concerns arise from fears of potential harm, loss of control, or exploitation from further breaches. As a result, they may have lower levels of trust in service providers or organizations, due to heightened concerns about the security and confidentiality of their information (Krasnova et al., 2012). As also posited by Yeh et. al (2018), individual experiences with privacy invasions can shape one's general belief system and willingness to share personal information. Empirical studies in e-commerce have shown that experiencing privacy invasions is positively related to increased information privacy concerns and indirectly affects consumer trust (Yeh et al., 2018).

In addition, other studies also support the mediating role of privacy concerns in the relationship between self-efficacy and trust (Tronnier et al., 2022). High self-efficacy leads to lower privacy concerns, which subsequently enhances trust in m-commerce apps. Users with higher self-efficacy are more capable of managing privacy settings, which reduces their privacy concerns. They are better equipped to understand and control their privacy settings and data-sharing behaviors within the app. This capability can lead to

lower privacy concerns because these users feel more confident in managing their privacy (Compeau et al., 1999; Shih et al., 2012). Consequently, lower privacy concerns can enhance trust in an app, as individuals perceive it as more secure. Additionally, individuals with higher self-efficacy experience fewer privacy concerns when using online platforms, which in turn increases their trust in these platforms (Chen, 2018). Additionally, self-efficacy in using technology reduced privacy concerns and enhanced trust in e-commerce environments (Aivazpour & Rao, 2020).

In this study context, this study believed that the role of privacy concerns as a mediator among app permission concerns, privacy awareness, privacy experience, self-efficacy, and trust highlights the complex interplay of factors that influence individuals' perceptions of privacy and trust in m-commerce apps among consumers in Malaysia. Therefore, the hypotheses were constructed as below:

H6a: Privacy concerns mediate the relationship between app permission concerns and trust.
H6b: Privacy concerns mediate the relationship between privacy awareness and trust.
H6c: Privacy concerns mediate the relationship between privacy experience and trust.
H6d: Privacy concerns mediate the relationship between self-efficacy and trust.

3. METHODOLOGY

3.1 Theoretical and Underpinning Theories

The "Antecedents ➔Privacy Concerns ➔Outcomes" (APCO) framework has been referred to and recommended by previous researchers in studying the area of information privacy (Dinev *et al*., 2015; Kaushik *et al*., 2018; Lin & Filieri, 2015; Ozdemir *et al*., 2017; Veltri & Ivchenko, 2017; Wang *et al*., 2019; Yeh *et al*., 2018; Zhang *et al.*, 2016), based on Smith et al. (2011). Hence, this study employs the "Antecedents Privacy Concern Outcomes" (APCO) framework to fit the current study in solving the problem stated.

Smith et al. (1996) conducted an interdisciplinary assessment of privacy research that is frequently cited. The review took into account and conceptualized studies relating to privacy from a wide range of disciplines, including political science, information systems, marketing, law, social science, psychology, and economics. The researchers looked at almost 130 books, parts, and less than 350 articles that were published from early 1961 until 2014s. After being studied for several years, the scholars concluded that almost all privacy related to empirical research can be viewed through the "Antecedents ➔Privacy Concerns ➔Outcomes" (APCO) (APCO) Framework. Hence, below is an explanation of the APCO framework to help understand the whole framework (Smith et al., 2011). Information privacy literature that emphasizes the disclosure of personal data as the key outcome variable presents and reviews issues of privacy related to outcomes in association with the "Antecedents ➔Privacy Concerns ➔Outcomes" (APCO) framework (Belanger & Crossler, 2011; Elhaj, 2011; Smith *et al*., 2011). In this study, PC → O represents privacy concerns regarding the usage of mobile applications. The expected outcome of this study is trust.

A consequentialist trade-off of costs and benefits that affects a person's behavioral responses is known as the privacy calculus. These views have been documented in a number of publications (Carlsson Hauff & Nilsson, 2021; Chatterjee, Chaudhuri, Vrontis, & Hussain, 2022; Chatterjee, Chaudhuri, Vrontis, & Siachou, 2022; L. Wang et al., 2020). The cost-benefit trade-off analysis used in this study serves as the foundation for the

privacy calculus theory, which holds that people make privacy decisions based on their perceptions of the advantages and disadvantages of information-sharing behavior (Gouthier et al., 2022; Jozani et al., 2020). (Dinev & Hart, 2006; Sun et al., 2015). Studies have shown that although people can choose to share their data and information, they can also choose to withhold it under some conditions (Keith, Babb, et al., 2016; Mohammed, 2017; Ozturk et al., 2017).

In this study, antecedents such as app permission concerns, privacy awareness, and privacy experience significantly shape privacy concerns (Smith et al., 2011; Gu et al., 2017). For instance, individuals with high privacy awareness and prior negative experiences with app permissions may develop heightened privacy concerns. Hence, privacy concerns, in turn, mediate the impact of these antecedents on the outcome (Joseph, 2017). By providing a clear framework, the APCO model ensures a systematic examination of how various factors influence consumer behavior (Sun et al., 2019). Besides, trust plays a critical role in interactions and is significant for firms to develop relationships with consumers (Alzaidi & Agag, 2022).

Consumers can use the privacy calculus to determine whether or not they wish to disclose their data based on the outcomes of a calculation called a trade-off analysis, which weighs the advantages and disadvantages of disclosure requirements and privacy concerns in a particular information-disclosure context (Wang *et al*., 2016). The concept of calculus, which holds that personal information is provided in return for specific advantages, serves as the foundation for individual privacy decisions (Yang et al., 2020). Moreover, privacy calculus has been the theory most frequently used by earlier scholars to address privacy-related concerns, according to Wirth et al. (2018). It has been applied to explain a dependent variable pertaining to privacy concerns around three times. Information disclosure is first explained as a dependent variable using the privacy calculus. Since sharing information does not frequently compromise people's privacy, information disclosure is a crucial dependent variable (Wirth et al., 2018).

According to Dinev and Hart (2006) and Sun et al. (2015), the privacy calculus theory in this study is based on cost-benefit trade-off analysis, which means people make privacy decisions based on their assessments of the risks and rewards produced by the information disclosure behavior. Research has indicated that although people may be persuaded to divulge personal information, they may also opt to keep their information private in some situations (Keith et al., 2016; Mohammed, 2017; Ozturk et al., 2017). The privacy calculus is a tool that helps customers make decisions about data exposure based on the outcomes of a trade-off analysis, which weighs the advantages and disadvantages of disclosure requirements and privacy concerns in a particular information-disclosure situation (Wang *et al*., 2016). The concept of "calculus," in which personal information is exchanged for specific advantages, is the foundation of individual privacy decision-making (Chen, 2018).

As a result, one important concept drawn from Social Cognitive Theory (SCT) is self-efficacy. Underlying social change is characterized by perceptions about one's capacity to engage in a particular behavior (Mohamed & Ahmad, 2012). According to social cognitive theory, anxiety arousal is significantly influenced by an individual's self-efficacy in this study. According to this notion, threat is a reasonable assessment of one's perceived capacity for coping as well as a potentially challenging activity or situation. According to the study, people who think they can practice and exert control over possible risks would eventually feel significantly less anxious than people who think they can't adjust to their surroundings and cope with stress (Yao et al., 2007). Only app permission

concerns are tested in this study because they are essential to the anticipated outcomes. Regarding this study, users of mobile devices could potentially protect themselves by declining permission requests from apps that ask for access to personal information such as contacts, whereabouts, and other relevant data. According to this study, information privacy concerns about the exponential rise in mobile app usage and the resulting proliferation of app permissions are critical.

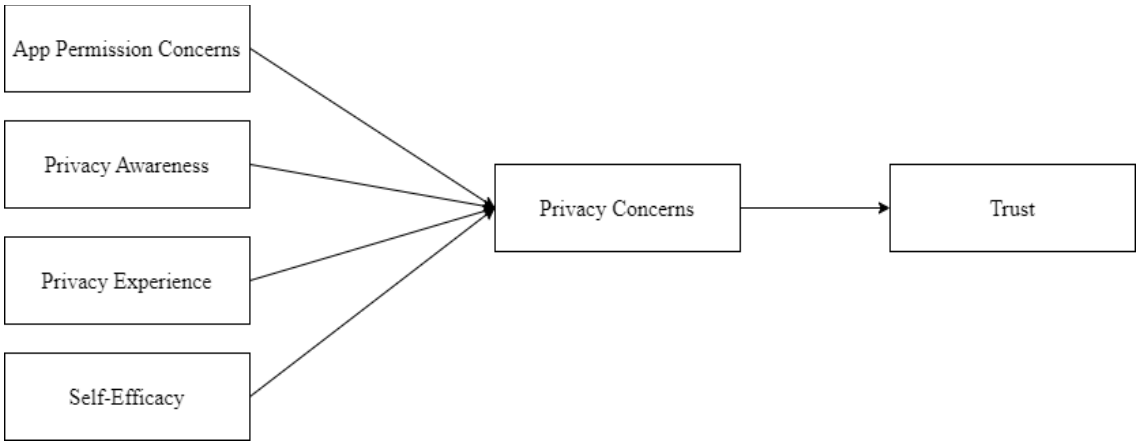

Figure 1: Proposed Conceptual Framework

3.2 Methods and Data

3.2.1 Measurement Scale and Instruments Development

The variables are operationalized using the Likert scale (Likert, 1932). The Likert scale has been widely used within the literature to measure variables or constructs within several contexts (Aiken, 2000; Chomeya, 2010; Gregory, 2003). The relevance of each item in the questionnaire was presented on a seven-point Likert scale: (1) strongly disagree, (2) disagree, (3) slightly disagree, (4) neutral, (5) slightly agree, (6) agree, and (7) strongly agree. In this study, a 7-point Likert scale was employed for measurement items to enhance the granularity and precision of the data collected. A 7-point scale offers a greater number of response options compared to a 5-point scale, enabling a more nuanced distinction in respondents' attitudes and perceptions (Allen & Seaman, 2007). Besides, Finstad (2010) pointed out that seven-point scales are more likely to reflect respondents' true subjective evaluation of a usability questionnaire item compared to five-point options. Research also supports that a 7-point scale can improve the reliability and validity of measurements by reducing central tendency bias and offering a wider range of response options (Taherdoost, 2019). This 7 Likert scale also aligns with respondent preferences by offering a neutral midpoint and preventing the need to choose extreme options. Consequently, the 7-point Likert scale was chosen to facilitate a more precise and detailed evaluation of the variables being studied. In addition, the use of a seven-point Likert scale was also one of the Likert scales supported in the information privacy literature (Offor, 2016; Dinev & Hart, 2006).

3.2.2 Sampling Techniques and Method Procedures

The purposive sampling technique is chosen after considering the factor of consumers as the target audience using mobile devices, especially m-commerce app(s). Prior to taking the survey, respondents are informed that m-commerce app(s) include all apps for which

they require disclosure of transaction information, and respondents are notified that the survey items are focused on their privacy concerns regarding m-commerce app(s) usage. This would help respondents have a clear understanding of how to view the survey questionnaire and provide a clear guideline for answering each questionnaire item (Fink, 2002).

In addition, Comrey and Lee (1992) have presented their version of guidelines for determining sample sizes, in which 50 samples is an inferior sample size, 100 samples is a poor sample size, 300 samples is a good sample size, 500 samples is a very good sample size, and 1000 samples is an excellent sample size (Comrey & Lee, 1992). Incidentally, Hair et al. (2016) suggested the use of the GPower tool to assess the minimum required sample size (Hair et al., 2016). As such, based on a medium effect size of 0.15, a significance level of 0.05, and a maximum of 10 predictors, the minimum sample size required for this research is 174 samples. In addition, a minimum of five observations also determined the sample size for the study (Hair et al., 2009). However, the sample size of 174, according to GPower, was relatively small and insufficient for the minimum requirement of sample size. Therefore, this study employed five-time observation, in which 58 measurements were multiplied by five (58 x 5 = 290), which is the minimum sample size for this study (Hair et al., 2016). As such, a total sample size of 292 was used in this study.

Besides, the frequency, measurement, and structural model of this study were analyzed using two pieces of software: Smart Partial Least Squares-based Structural Equation Modelling (PLS-SEM) and the Statistical Package for the Social Sciences version 28 (SPSS 28). The information gathered via the survey was examined and computed using the SPSS 28 template, utilizing Smart Partial Least Squares-based Structural Equation Modeling (PLS-SEM) for analysis. First, the use of partial least squares structural equation modeling for data analysis (PLS-SEM) is needed for analysis (Hair *et al*., 2016; Hair *et al*., 2014). A well-established approach in information systems and marketing research enables researchers to statistically and consistently examine the relationships between several independent and dependent variables at the same time (Ku & Chen, 2013). This approach involves two main stages.

Firstly, assess the measurement model, wherein the reliability and validity of the model’s measurement constructs are verified. Secondly, assess the structural model, wherein the model's hypotheses are tested. Data analysis was derived using SmartPLS software version 4.0 (Bawack *et al*., 2021). The following criteria are also taken into account while selecting PLS as the primary data analysis technique. PLS is a variance-based technique directed towards the model's predictive characteristics (variance explanation); PLS has modest sample size requirements; PLS does not presuppose multivariate normality and considers measurement errors while evaluating the structural model (Hair *et al*., 2017).

In this study, PLS-SEM is used to support the framework due to its ability to handle complex relationships and perform predictive analysis. With multiple constructs and intricate relationships involved, PLS-SEM's capability to manage and analyze these complexities makes it an ideal choice (Hair et al., 2011). This approach enables the researcher to examine how app permission concerns, privacy awareness, privacy experience, and self-efficacy influence privacy concerns, which serve as crucial mediators in the framework. Privacy concerns, in turn, were hypothesized to affect trust which was expected to mediate the relationship between app permission concerns, privacy awareness, privacy experience, and self-efficacy on trust. Additionally, the direct

effects of privacy concerns on trust were also examined. PLS-SEM supports this framework by enabling detailed analysis of both direct and indirect effects, which is crucial for understanding the pathways through which privacy concerns impact consumers' trust. Using the software SmartPLS, the analysis was conducted on the collected data. SmartPLS was selected for its user-friendly interface and robust features tailored for PLS-SEM, making it easier to implement and analyze the complex model (Hair *et al*., 2016; Hair *et al*., 2014). The bootstrapping technique provided significance testing for the path coefficients, revealing that privacy concerns had a significant positive impact on both trust and self-disclosure, contrary to the initial hypotheses. Bootstrapping is crucial in PLS-SEM as it allows for reliable significance testing of paths, supporting the robustness of the framework's findings (Hair et al., 2016).

4. RESULT AND FINDINGS

4.1 Respondents Profile

The frequency, measurement, and structural model of this study were analyzed using two pieces of software: Smart Partial Least Squares-based Structural Equation Modelling (PLS-SEM) and the Statistical Package for the Social Sciences version 28 (SPSS 28). The information gathered via the survey was examined and computed using the SPSS 28 template, utilizing Smart Partial Least Squares-based Structural Equation Modeling (PLS-SEM) for analysis. The SPSS(28) was used to analyze the respondent's profile as stated below.

The highest representation is located in Sabah state at 61%, while other states had lower percentages ranging from 0% to 7%. This distribution is influenced by factors like participant availability and response rates rather than intentional geographic targeting. States with higher participation, such as Sabah, Johor, and Selangor, may have larger populations or greater interest in the study, while those with lower participation might face logistical challenges. In terms of age, most respondents in this study were aged between 18 and 40, predominantly younger consumers. This age group is typically more proficient with technology and comfortable using mobile devices, which explains their higher engagement with m-commerce apps. Younger individuals are often more inclined to participate in online surveys and are usually early adopters of new technologies, eagerly exploring and benefiting from the convenience of mobile shopping. Besides, most respondents in this study reported moderate to high-income levels, which greatly impacted their engagement with m-commerce apps. Individuals with higher incomes have more disposable income, allowing for more frequent and varied purchases. They are more apt to invest in premium app features or subscription services, which enhances their experience and leads to increased use of m-commerce platforms.

Nonetheless, respondents in this study hold at least a bachelor's degree with 47.6%, indicating a higher level of digital literacy and comfort with technology. The distribution of occupations among respondents provides valuable insights into their engagement with m-commerce apps across different job categories. Notably, 27.4% work in the private sector, representing a significant demographic with steady incomes and busy lifestyles. Similarly, 25.7% are employed in government sectors, another major group that values the convenience and security of m-commerce platforms, often prioritizing reliability and accessibility for online purchases. Additionally, 24.0% are students, a tech-savvy group that relies heavily on mobile devices for various needs, including shopping. Students appreciate the flexibility and accessibility of m-commerce apps for both academic and personal use.

4.2 Common Variance Method (CMB)

This research also tested for common method bias, employing Harman's Single Factor test to check for its presence. Despite following procedural precautions during data collection, statistical results are recommended to support these measures (Mackenzie & Podsakoff, 2012). The Harman's Single Factor test showed that the first factor explained only 27% of the total variance, well below the 50% cut-off, suggesting that common method bias is not a concern. However, some critics argue that this test is "weak and conceptually flawed" (Min et al., 2016) as it does not control for method variance but only checks if one factor explains the majority of variance.

To address this limitation, the study also used a full collinearity test with Variance Inflation Factor (VIF) values, as proposed by Kock (2015), to further assess common method bias. A VIF value of 5 or higher suggests high multicollinearity, indicating potential redundancy among predictors (Hair et al., 2011). This study showed that the value for VIF is less than the value of 5, indicating the absence of multicollinearity as shown in Table 1. In addition, to address social desirability bias in the study, anonymity and confidentiality were implemented. Providing anonymity in self-administered questionnaires reduces social pressure and the tendency to give socially desirable responses (Krosnick & Presser, 2009). The study ensured that responses were anonymous and clearly communicated that they would remain confidential and used solely for research purposes. Additionally, pre-tests and pilot studies were conducted to refine survey questions and methods, helping to identify and correct questions that might lead to socially desirable answers (Dillman, 2000). This approach helps ensure that the final survey captures genuine responses, improving the study's validity and minimizing social desirability effects (Creswell & Creswell, 2017).

Table 1: VIF Collinearity

Constructs	VIF
AP	1.113
PA	1.224
PC	1.000
PE	1.024
SE	1.225

4.3 Measurement Model Testing

To ensure the reliability and validity of the measurement model in PLS-SEM comprehensively, various methods are employed for this study. These include evaluating Composite Reliability (CR) to measure internal consistency, assessing Average Variance Extracted (AVE) to confirm convergent validity, and examining factor loadings to verify the strength of item-construction relationships. Additionally, discriminant validity is checked to ensure that constructs are distinct from one another, using criteria such as the Fornell-Larcker criterion or the Heterotrait-Monotrait Ratio (HTMT). These methods collectively provide a comprehensive assessment of the measurement model's robustness and accuracy (Hair et al., 2014; Hair et al., 2016).

Internal reliability can be assessed using Cronbach's alpha and composite reliability, whereas convergent validity can be assessed using factor loading and average variance extracted. As indicated in Table 2, the Cronbach's alpha and composite reliability values for the six latent variables above the suggested threshold of 0.7, indicating that the results

were reliable (Hair et al., 2016) The convergent validity examines the values of factor loadings and weights of items, as well as the average variance extracted (AVE) of constructs, to determine the extent to which items for the same construct are associated (Hair et al., 2016). According to Table 2, the factor loadings of items from most of the reflective variables (at a significant level of p 0.001) were above the required threshold of 0.7, and the AVE of all constructs was greater than 0.5 (Hair Jr et al., 2016).

Standardized factor loadings of measuring items, as well as average variance extracted (AVE) and composite reliability (CR) of the latent construct, can be used to assess convergence validity. Items on the measuring scale must produce standardized loadings (on their related construct) greater than 0.5, according to Hair et al. (2016). As shown in Table 2, all measurement scale items meet this condition, with standardized loadings of at least 0.742. These statistics provide preliminary evidence for the convergent validity hypothesis. It also demonstrates that the AVE and CR for each latent concept are greater than the threshold values of 0.5 (Fornell and Larcker, 1981) and 0.7 (Nunnally, 1978), indicating that convergent validity is well established.

In general, discriminant validity is examined in this study using two methods: cross-loading and the Fornell-Larcker criterion. As a result, this study employed the latest technique proposed by Henseler et al. (2015), which is based on the multitrait-multimethod matrix and employs the heterotrait-monotrait ratio of correlations (HTMT). First, the discriminant validity of all items for all constructs is evaluated using their cross-loading values. According to Hair et al. (2016), when compared to its cross-loading with other constructions, the outer loadings of an indicator on a construct should be more than 0.1. Table 3 displays the cross-loading values for all items in this study. The following table shows that the outer loadings of each construct are greater than 0.1 when compared to their cross-loadings, implying discriminant validity. To examine the discriminant validity of the constructs, the Fornell-Larcker criterion was utilized in its traditional form. The Fornell-Larcker criterion results for the constructs in this investigation are shown in Table 4. The findings demonstrate that the square of the AVE for each construct is greater than its connection with other constructs. As a result, cross-loadings support the proven discriminant validity (Hair et al., 2016; Ramayah et al., 2018).

Table 2 serves as a pivotal testament to the robust discriminant validity of this measurement construct, showcasing HTMT ratios consistently below the esteemed threshold of 0.85 (Henseler et al., 2015). This compelling empirical support underscores the precision and reliability of this analytical framework. In challenging the conventional tools for discerning discriminant validity, Henseler et al. (2015) argue that the Fornell-Larcker criterion and cross-loading may falter in common research scenarios. This study adopts a forward-thinking approach by embracing the Heterotrait-Monotrait (HTMT) method, a choice vindicated by the method's superior performance in a Monte-Carlo simulation study (Henseler et al., 2015). Table 5, a canvas of methodological excellence, presents the outcomes of this HTMT approach. Notably, none of the HTMT values surpass the 0.9 threshold across any constructs, affirming the discriminant validity of this model. This echoes the insights of Henseler et al. (2015) and Ramayah et al. (2018), further elevating the confidence in the credibility of these findings within the scholarly discourse.

Table 2: Internal Consistency Reliability and Convergent Validity

Construct	Item	Indicator Reliability	Convergent Validity	Internal Reliability	Consistency
		Loadings	**AVE[a]**	**Composite Reliability**	**Cronbach's Alpha (α)**
Privacy Concerns	PC2	0.729	0.724	0.971	0.970
	PC3	0.718			
	PC4	0.746			
	PC5	0.878			
	PC6	0.866			
	PC7	0.912			
	PC8	0.911			
	PC9	0.909			
	PC10	0.885			
	PC11	0.898			
	PC12	0.855			
	PC13	0.847			
	PC14	0.878			
	PC15	0.849			
App Permission Concerns	APC1	0.890	0.798	0.937	0.879
	APC2	0.911			
	APC3	0.879			
Privacy Awareness	PA2	0.818	0.738	0.854	0.826
	PA3	0.892			
	PA4	0.866			
Privacy Experience	PE2	0.857	0.742	0.906	0.836
	PE3	0.843			
	PE4	0.883			
Self-Efficacy	SE5	0.755	0.623	0.887	0.879
	SE6	0.780			
	SE7	0.820			
	SE8	0.789			
	SE9	0.824			
	SE10	0.762			
Trust	TRU1	0.816	0.930	0.676	0.885
	TRU2	0.810			
	TRU3	0.862			
	TRU4	0.847			
	TRU5	0.774			

Table 3: Cross Loadings

	ADB	AP	PA	PC	PE	SE	TRU
AP1	0.227	0.889	0.193	0.249	-0.019	-0.185	0.031
AP2	0.251	0.910	0.174	0.272	0.027	-0.205	0.022
AP3	0.135	0.879	0.260	0.407	-0.005	-0.317	0.123
PA2	0.097	0.168	0.818	0.316	-0.075	-0.284	0.149
PA3	0.063	0.211	0.892	0.426	-0.080	-0.338	0.138
PA4	0.148	0.236	0.866	0.488	-0.204	-0.346	0.233
PC2	0.179	0.377	0.364	0.723	-0.043	-0.358	0.268
PC3	0.161	0.373	0.369	0.711	-0.028	-0.403	0.260
PC4	0.192	0.388	0.323	0.740	-0.044	-0.439	0.248
PC5	0.247	0.312	0.435	0.877	-0.161	-0.415	0.326
PC6	0.239	0.308	0.415	0.865	-0.195	-0.412	0.306
PC7	0.228	0.308	0.435	0.912	-0.218	-0.429	0.358
PC8	0.188	0.304	0.463	0.912	-0.200	-0.444	0.333
PC9	0.279	0.309	0.435	0.911	-0.169	-0.462	0.381
PC10	0.258	0.316	0.406	0.887	-0.142	-0.398	0.333
PC11	0.254	0.304	0.464	0.900	-0.190	-0.442	0.367
PC12	0.193	0.270	0.397	0.859	-0.183	-0.394	0.332

PC13	0.229	0.258	0.457	0.851	-0.182	-0.405	0.360
PC14	0.230	0.276	0.442	0.881	-0.251	-0.430	0.390
PC15	0.229	0.288	0.411	0.852	-0.163	-0.432	0.359
PE2	0.128	0.052	-0.102	-0.151	0.857	0.086	-0.237
PE3	0.207	0.025	-0.096	-0.096	0.844	0.048	-0.161
PE4	0.140	-0.049	-0.164	-0.201	0.883	0.038	-0.173
SE5	-0.125	-0.185	-0.276	-0.374	0.068	0.760	-0.181
SE6	-0.102	-0.230	-0.225	-0.321	0.046	0.792	-0.192
SE7	-0.219	-0.251	-0.383	-0.414	0.085	0.816	-0.218
SE8	-0.180	-0.220	-0.258	-0.350	0.000	0.791	-0.287
SE9	-0.105	-0.232	-0.293	-0.354	0.059	0.829	-0.232
SE10	-0.219	-0.204	-0.341	-0.488	0.045	0.749	-0.298
TRU1	0.252	0.042	0.135	0.231	-0.187	-0.168	0.825
TRU2	0.311	0.160	0.226	0.449	-0.182	-0.293	0.787
TRU3	0.269	0.076	0.186	0.369	-0.165	-0.273	0.856
TRU4	0.324	0.014	0.149	0.280	-0.148	-0.242	0.860
TRU5	0.300	-0.021	0.126	0.205	-0.245	-0.226	0.799

Table 4: Fornell-Larcker Criterion

	AP	PA	PC	PE	SE	TRU
AP	**0.893**					
PA	0.244	**0.859**				
PC	0.365	0.490	**0.851**			
PE	0.001	-0.148	-0.187	**0.861**		
SE	-0.279	-0.380	-0.492	0.065	**0.790**	
TRU	0.077	0.207	0.390	-0.222	-0.300	**0.826**

Table 5: HTMT Ratio

	AP	PA	PC	PE	SE	TRU
AP						
PA	0.267					
PC	0.378	0.532				
PE	0.060	0.156	0.190			
SE	0.299	0.434	0.527	0.089		
TRU	0.099	0.227	0.398	0.259	0.327	

4.4 Structural Model Testing

After completion of the measurement model analysis using the reflective measurement analysis, the structural model of the research can be started (Becker *et al*., 2012). In this step, a bootstrapping procedure using non-parametric methods is, which allows the testing of statistical significance of different results in PLS-SEM such as path coefficients, composite reliability, HTMT, and R2 values (Hair *et al*., 2014). In order for the bootstrapping procedure to proceed, the researcher must specify a certain number of subsamples (i.e.) that will be randomly drawn from the original data set. Specifically, this research would employ 5000 subsamples for the bootstrapping procedure.

The hypotheses were tested by measuring their significant levels and path coefficients using the Bootstrap method (5000 subsamples). The R2 value was applied to explain the percentage of variance contributed by the independent variables in the proposed model. Table 6 shows the results of the hypotheses testing. According to the results, APC (β =0.204, $p < 0.000$), PA ($\beta = 0.304$, $p < 0.000$), PE ($\beta = -0.122$, $p < 0.003$), SE ($\beta = -0.312$, $p < 0.000$) had significant effects on PC. Therefore, H1, H2, H3, and H4 were accepted. The results also showed that PC ($\beta = 0.390 < p, 0.000$) had a significant effect on TRU. Hence, H5 was also accepted.

The f^2 calculates the relative impact of a predictor construct on endogenous constructs. According to Sullivan and Feinn (2012), besides reporting the p-value, both the substantive significance (effect size) and statistical significance (p-value) are of crucial importance. A guideline from Cohen (1988) is followed to measure the effect size. Based on Cohen (1988), 0.02, 0.15, and 0.35 represent small, medium, and large effects.

The hypotheses were tested by measuring their significant levels and path coefficients using the Bootstrap method (5000 subsamples). Table 7 shows the results of the mediation testing. According to the results, this study found that the effect of APC on TRU was fully mediated by PC (β =0.080, $p < 0.000$), PC was fully mediated the relationship between PA and TRU ($\beta = 0.119$, $p < 0.000$), PC was fully mediated the relationship between PE and TRU ($\beta = -0.048$, $p < 0.003$) and PC was also fully mediated the relationship between SE and TRU ($\beta = -0.122$, $p < 0.000$). Therefore, H6a, H6b, H6c and H6d were also

supported. The results suggested that H6a (β=0.080, t=3.660, UL=0.045 LL=0.116), H6b (β=0.119, t=3.459, UL=-0.065, LL=0.177), H6c (β=-0.048, t=2.279, UL=-0.080, LL=-0.024), and H6d (β=-0.122, t=3.319, UL=-0.189, LL=-0.067) were accepted.

Table 6: Direct Relationship Testing

Hypotheses	Path	Beta (β)	T-Value	P-Value	f^2	LL	UL
H1	APC > PC	0.204	4.249	0.000	0.062	0.123	0.281
H2	PA > PC	0.304	4.423	0.000	0.126	0.183	0.411
H3	PE > PC	-0.122	2.769	0.003	0.024	-0.201	-0.061
H4	SE > PC	-0.312	5.090	0.000	0.133	-0.419	-0.216
H5	PC > TRU	0.390	5.927	0.000	0.180	0.311	0.509

Table 7: Mediation Testing

Hypotheses	Path	Beta (β)	T-Value	P-Value	LL	UL
AP	APC > PC > TRU	0.080	3.660	0.000	0.048	0.119
PA	PA > PC > TRU	0.119	3.459	0.000	0.069	0.180
PC	PE > PC > TRU	-0.048	2.279	0.003	-0.082	-0.025
PE	SE > PC > TRU	-0.122	3.319	0.000	-0.195	-0.075

5. DISCUSSION

This study looked at the association between app permission concerns, privacy awareness, privacy experience, and self-efficacy regarding privacy concerns. A number of inferences can be drawn from this investigation.

This study posited that (H1), (H2), (H3), and (H4) were supported. This study confirmed that app permission concerns (H1) positively influenced privacy concerns. In Malaysia, where m-commerce is mainly information-based, transparent privacy policies enhance understanding of data practices without significantly affecting acceptance rates. The study highlights the importance of clear privacy disclosures in mobile permissions and provides guidelines for creating privacy-transparent apps. (H2) was also found to be significantly influenced by privacy concerns. This aligns with previous research indicating that higher privacy awareness leads to greater privacy concerns in the context of mobile usage (Belanger et al., 2019; Škrinjarić et al., 2018; Soumelidou & Tsohou, 2020; Warner & Wang, 2019). In Malaysia, increased privacy awareness helps consumers recognize potential privacy breaches and adjust their privacy settings, leading them to be more cautious about sharing personal information when using m-commerce apps (Soumelidou & Tsohou, 2020).

However, this study found a positive relationship between privacy experience (H3) and privacy concerns. This unexpected finding indicates that, contrary to the hypothesis, increased privacy experience does not lead to higher privacy concerns. Several explanations may account for this outcome. One possibility is that as consumers gain more experience with privacy issues, they become better equipped to manage and mitigate these concerns, leading to a reduction in overall privacy anxiety. This improved capability could result in a more nuanced understanding of privacy, where individuals feel more in control and less concerned about potential privacy risks (Chen & Chen, 2015; Giwah *et al*., 2020). Additionally, it is possible that with greater privacy experience, users become more adept at identifying and avoiding apps or practices that pose privacy risks, thereby reducing their overall level of concern. This experience may also lead to a more balanced

perspective on privacy issues, where consumers are able to differentiate between actual risks and perceived threats, ultimately diminishing their privacy concerns (Škrinjarić *et al*., 2018; Tseng *et al*., 2023). Overall, this finding suggested that privacy experience may play a role in reducing privacy concerns, highlighting the need for further research to explore how experience and expertise in privacy management influence users' perceptions and behaviors.

Nonetheless, this study also found that (H4) would negatively influence privacy concerns. This is in line with a prior study previously in the mobile usage context (Belanger et al., 2019; Butler, 2020; Chen, 2018; Giwah et al., 2020; Wang et al., 2019). In this study, higher self-efficacy in data protection was associated with fewer privacy concerns among Malaysian consumers using m-commerce apps. Individuals with high self-efficacy are more confident in managing their data and navigating technology, leading to reduced privacy concerns. Self-efficacy affects how people respond to uncertainty and challenges, influencing their engagement and ability to overcome barriers (Chang et al., 2022; Mamonov & Benbunan-Fich, 2018).

The results also indicated that privacy concerns mediate the relationship between app permission concerns, privacy awareness, privacy experience, and self-efficacy on trust, thus supporting hypotheses of (H6a), (H6b), (H6c), and (H6d). These imply that the effect of app permission concerns (H6a) on trust is mediated through privacy concerns. This study is in line with a study by Hsieh and Li, (2022); Walter and Albendroth (2020); Chong and Ma (2021); (Momenzadeh et al., 2021)., posited that when users are more concerned about app permissions, their overall privacy concerns increase, which then impacts their trust in the app. This mediation effect highlights the necessity of addressing privacy concerns to build trust. It suggested that consumers' trust in an app is influenced not only by the permissions requested but also significantly by the privacy concerns associated with those permissions (Hsieh & Li, 2022). Meanwhile, (H6b) indicated that increased awareness of privacy issues such as data collection, sharing policies, and security risks would likely intensify privacy concerns, which in turn affects users' trust in the app (Chong & Ma, 2021). In m-commerce, where sensitive data is often handled, heightened privacy awareness leads users to evaluate the app's privacy protections and transparency. Apps that effectively address privacy concerns can build and enhance consumer trust. (H6c) was also found to be significant and supported.

(H6b) revealed that increased awareness of privacy issues such as data collection, sharing policies, and security risks intensifies privacy concerns, which in turn affects users' trust in the app (Chong & Ma, 2021). In m-commerce, where sensitive data is often handled, heightened privacy awareness leads users to evaluate the app's privacy protections and transparency. Apps that effectively address privacy concerns can build and enhance consumer trust. Nonetheless, this study also revealed that (H6c) was significant. This aligns with Baker-Eveleth et al. (2022) and Ayaburi (2022), which found that heightened privacy awareness leads individuals to scrutinize how apps manage their data, affecting their trust. As consumers gain more privacy experience, their expectations for privacy management become more stringent. Thus, m-commerce apps need to address privacy issues and clearly communicate their privacy measures to build and maintain trust. This study also found that (H6d) was significant. When Consumers are more concerned about app permissions, their overall privacy concerns rise, which affects their trust in the app. This emphasizes the need to address privacy concerns to build trust. Research shows that consumers' trust is influenced by both app permissions and related privacy concerns (Hsieh & Li, 2022). Increased awareness of privacy issues also

heightens concerns and impacts trust (Chong & Ma, 2021). In m-commerce, where sensitive data is handled, effective privacy management and communication can enhance trust.

5.1 Theoretical Implications

In theory, this research advances an understanding of how consumers make privacy-related decisions. This study also gave a fresh perspective on personalisation-privacy conflict, notably when using mobile phones to disclose personal data such as name, address, and financial transactions on m-commerce app(s). This study is unique from others since it combined the Social Cognitive Theory (SCT) and the APCO framework into a single framework to enhance earlier research. In determining consumers' trust, this study also adds to the relationship between Social Cognitive Theory (SCT) and APCO & (app permission concerns). SCT and APCO & (app permission concerns) haven't been presented in an integrated model alongside the theme of m-commerce app(s) in one framework very often. To present the full structure, SCT and APCO & (app permission issues) are used as theories. Through a unique relationship between app permission concerns, privacy awareness, privacy experience, self-efficacy, privacy concerns, and trust, the association between SCT and APCO (app permission concerns) has strengthened the framework that could explain the privacy paradox of consumers' trust towards the usage of the m-commerce platform. Nonetheless, this study also focused on a region-specific context, Malaysia.

5.2 Practical Implications

The practical implications of this study provide significant implications for organizations, policymakers, and consumers. For organizations, addressing privacy concerns effectively can build stronger consumer trust, which is crucial for user engagement and retention. By implementing robust privacy protections and transparent data practices, organizations can meet consumers' heightened privacy expectations, thereby enhancing their trust in the platform (Saxborn et al., 2024). Additionally, the study highlights the importance of designing privacy features that do not inadvertently reduce trust, even among more experienced consumers. This insight allows organizations to tailor their privacy management practices more efficiently. Besides, consumers would also benefit from these practical implications through improved privacy protection and increased trust in digital transactions. As m-commerce platforms address privacy concerns more effectively, consumers can enjoy enhanced transparency and robust privacy measures, leading to greater security and confidence in their interactions with these platforms (Zaini et al., 2024). Furthermore, better privacy controls and educational resources enable consumers to manage their privacy more effectively, resulting in a more positive and secure experience in the digital marketplace (Mutimukwe et al., 2020).

For policymakers, the study offers valuable insights for crafting informed privacy regulations. Policymakers can use these findings to develop regulations that require m-commerce platforms to enhance privacy protections and transparency, ensuring alignment with users' expectations and concerns. Supporting privacy education initiatives is also crucial, as it empowers users to manage their privacy effectively. Encouraging best practices in privacy management through guidelines or incentives can further promote effective privacy practices across the industry (Handoyo, 2024). Overall, by responding to these findings, organizations can improve user trust, policymakers can create

supportive regulatory frameworks, and consumers can experience enhanced privacy protection and confidence in their digital interactions (Jaspers & Pearsons, 2022).

5.3 Limitations

There are a number of limitations to this study that might be discussed from a wider angles. The breadth and depth of the results constitute the first constraint. Future investigations of the study's breadth may concentrate on particular demographics, including young teens or Generation Z. The sample size is one more way that this study is limited. Only 292 people made up the sample size in the current study. Future studies need to have a defined goal that is manageable.

Time and money restrictions were two of the study's shortcomings. The technique used in this investigation to collect data is another flaw. The questionnaire employed in this study was the only tool used to gather data. According to the current study, qualitative interviews should be utilized to gather information on the main factors or antecedents of consumers' behavior with regard to the adoption of mobile apps. This is a result of certain respondents' unwillingness to take part in the interview. Therefore, distributing questionnaires is a more effective technique to gather information and data. Finding enough literature to address every variable is another obstacle. Studies that include every characteristic related to app permission concerns, privacy awareness, privacy experience, self-efficacy, privacy concerns, and trust in the use of m-commerce apps in Malaysia, for instance, are non-existent (Chatterjee et al., 2021).

6. CONCLUSION

This study provides valuable insights into the dynamics between privacy concerns, app permission concerns, privacy awareness, privacy experience, and self-efficacy in influencing trust within m-commerce apps adding a novelty to the current research. The significant findings highlighted that app permission concerns, privacy awareness, and self-efficacy all play important roles in shaping trust through their effects on privacy concerns. Specifically, privacy experience (H3) demonstrated a unique negative relationship with privacy concerns, indicating that past negative experiences can diminish current privacy concerns. This result suggested that consumers with previous privacy invasions may become more resilient or less sensitive to privacy concerns in their current interactions with m-commerce apps. This indicates that past experiences with privacy invasions may lead to greater resilience or adaptation, where individuals become less concerned or more accepting of privacy risks in their current interactions with m-commerce apps among consumers in Malaysia.

Besides that, users who have previously encountered privacy breaches may develop a more pragmatic approach to managing privacy risks. For m-commerce platforms, this means that privacy strategies should be tailored to address the specific concerns of users with varying privacy experiences. These users might need more robust privacy protections to feel secure. This finding extends existing privacy theories by highlighting the impact of past privacy experiences on current perceptions, offering deeper insights into the dynamics of privacy and trust. Practically, it underscores the need for clear and effective communication about privacy practices to build trust and satisfaction among users with different privacy matters (Baker-Eveleth, 2022).

Nonetheless, the study extends theoretical frameworks by integrating privacy experience into the analysis, providing a nuanced understanding of how past privacy issues impact current privacy perceptions and trust. In practical terms, the study highlights

that m-commerce platforms must prioritize transparent data practices and clear communication about privacy policies to build and maintain user trust. By addressing concerns related to privacy matters and enhancing the overall privacy experience, platforms can foster a more trustworthy relationship with their users. These insights are crucial for both academic researchers and practitioners seeking to understand and improve trust in the m-commerce sector (Gouthier et al., 2022). In addition, this result not only enhances the understanding of how historical privacy issues influence current privacy perceptions but also highlights the importance of implementing robust privacy protections and clear communication to build trust. By addressing these varied privacy needs, platforms can better manage user trust and satisfaction, particularly for those who have previously encountered privacy breaches.

REFERENCES

Aiken, R. (2000). Psychological Testing and Assessment. In *Boston: Allyn and Bacon*.

Allen, I. E., & Seaman, C. A. (2007). Likert scales and data analyses. *Quality progress*, *40*(7), 64-65.

Aivazpour, Z., & Rao, V. S. (2020). Information disclosure and privacy paradox: The role of impulsivity. *Data Base for Advances in Information Systems*, *51*(1), 14–36.

Akhter, S. H. (2014). Privacy concern and online transactions: The impact of internet self-efficacy and internet involvement. *Journal of Consumer Marketing*, *31*(2), 118–125.

Alzaidi, M. S., & Agag, G. (2022). The role of trust and privacy concerns in using social media for e-retail services: The moderating role of COVID-19. *Journal of Retailing and Consumer Services*, *68*(May), 103042.

Anic, I. D., Škare, V., & Kursan Milaković, I. (2019). The determinants and effects of online privacy concerns in the context of e-commerce. *Electronic Commerce Research and Applications*, *36*(June).

Ayaburi, E. W. (2022). Understanding online information disclosure: examination of data breach victimization experience effect. *Information Technology and People*, *36*(95–114).

Baker-Eveleth, L., Stone, R., & Eveleth, D. (2022). Understanding social media users' privacy-protection behaviors. *Information and Computer Security*, *30*(3), 324–345.

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*(November 2019), 102063.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. Information & Management, *53*(1), 1–21.

Bawack, R. E., Wamba, S. F., & Carillo, K. D. A. (2021). Exploring the role of personality, trust, and privacy in customer experience performance during voice shopping: Evidence from SEM and fuzzy set qualitative comparative analysis. *International Journal of Information Management*, *58*(December 2020).

Belanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1041.

Belanger, F., Crossler, R. E., & Pamplin, R. B. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *Journal of Strategic Information Systems*, 1–0.

Betzing, J. H., Tietz, M., vom Brocke, J., & Becker, J. (2019). The impact of transparency on mobile privacy decision making. *Electronic Markets*, *30*, 607–625.

Bhandari, S., Jaballah, W. Ben, Jain, V., Laxmi, V., Zemmari, A., Gaur, M. S., Mosbah, M., & Conti, M. (2017). Android inter-app communication threats and detection techniques. *Computers and Security*, *70*, 392–421.

Bhattacharya, S., Sharma, R. P., & Gupta, A. (2022). Does e-retailer's country of origin influence consumer privacy, trust and purchase intention? *Journal of Consumer Marketing*, *40*(2), 248–259.

Butler, R. (2020). A systematic literature review of the factors affecting smartphone user threat avoidance behaviour. *Information and Computer Security*, *28*(4), 555–574.

Carlsson Hauff, J., & Nilsson, J. (2021). Individual costs and societal benefits: the privacy calculus of contact-tracing apps. *Journal of Consumer Marketing*, *2*(July 2021), 171–180.

Chatterjee, S., Chaudhuri, R., Vrontis, D., & Hussain, Z. (2022). Usage of smartphone for financial transactions: from the consumer privacy perspective. *Journal of Consumer Marketing*, *40*(2), 193–208.

Chatterjee, S., Chaudhuri, R., Vrontis, D., & Siachou, E. (2022). Examining the dark side of human resource analytics: an empirical investigation using the privacy calculus approach. *International Journal of Manpower*, *43*(1), 52–74.

Chen, H. T. (2018). Revisiting the Privacy Paradox on Social Media With an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management. *American Behavioral Scientist*, *62*(10), 1392–1412.

Chen, H. T., & Chen, W. (2015). Couldn't or wouldn't? the influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13–19.

Cheng, Z., Li, K., & Teng, C. I. (2022). Understanding the influence of privacy protection functions on continuance usage of push notification service. *Aslib Journal of Information Management*, *74*(2), 202–224.

Chomeya, R. (2010). Quality of psychology test between Likert scale 5 and 6 points. *Journal of Social Sciences*, *6*(3), 399-403.

Chong, W. K., & Ma, Z. (2021). The quality of user experiences for mobile recommendation systems: an end-user perspective. *Industrial Management and Data Systems*, *121*(5), 1063–1081.

Chopdar, P. K., Korfiatis, N., Sivakumar, V. J., & Lytras, M. D. (2018). Mobile shopping apps adoption and perceived risks: A cross-country perspective utilizing the Unified Theory of Acceptance and Use of Technology. *Computers in Human Behavior*, *86*, 109–128.

Cloarec, J. (2022). Privacy controls as an information source to reduce data poisoning in artificial intelligence-powered personalization. *Journal of Business Research*, *152*(July), 144–153.

Cohen, J. 1988. Statistical Power Analysis for the Behavioural Science. New Jersey: Erlbaum.

Compeau, D., Higgins, C. A., & Huff, S. (1999). Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study. *MIS Quarterly*, *23*(2), 145.

Compeau, D. R., & Higgins, C. A. (1995). Application of Social Cognitive Theory to Training for Computer Skills. *Information Systems Research*, *6*(2), 118–143.

Comrey, A. L., & Lee, H. B. (1992). A first course in factor analysis. Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

Correia, J., & Compeau, D. (2017). Information Privacy Awareness (IPA): A Review of the Use, Definition and Measurement of IPA. *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*, 4021–4030.

Creswell. J.W. and Creswell, J.D. (2017) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 4th Edition, Sage, Newbury Park.

Degirmenci, K. (2020). Mobile users ' information privacy concerns and the role of app permission requests. *International Journal of Information Management*, *50*(May 2019), 261–272.

Dillman, D.A. (2000) Mail and Internet Surveys: The Tailored Design Method. 2nd Edition, John Wiley and Sons, New York.

Dinev, T. (2014). Why would we care about privacy? *European Journal of Information Systems*, *23*(2), 97–102.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour and Information Technology*, *23*(6), 413–422.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Transactions Model for. *Information Systems Research*, *17*(1), 61–80.

Dinev, T., Mcconnell, A. R., & Smith, H. J. (2015). Economics : Thinking Outside the " APCO " Box Systems , Psychology , and Behavioral Economics : Thinking Outside the " APCO " Box. *Information Systems Research*, *26*(4), 639–655.

Distler, V., Lallemand, C., & Koenig, V. (2020). How Acceptable Is This? How User Experience Factors Can Broaden our Understanding of The Acceptance of Privacy Trade-offs. *Computers in Human Behavior*, *106*, 106227.

Dogruel, L., Joeckel, S., & Henke, J. (2023). Disclosing Personal Information in mHealth Apps. Testing the Role of Privacy Attitudes, App Habits, and Social Norm Cues. *Social Science Computer Review*, *41*(5), 1791–1810.

Elhaj, M. (2011). CONSUMERS'PERCEPTIONS TOWARD ONLINE AND TRADITIONAL FLIGHT RESERVATION METHODS IN THE U.S. In *Journal of Strategic Studies* (Vol. 34, Issue 2).

Finstad, K. (2010). Response Interpolation and Scale Sensitivity: Evidence Against 5-Point Scales. Usability Metric for User Experience, 5(3), 104-110.

Foltz, C. B., & Foltz, L. (2020). Mobile users' information privacy concerns instrument and IoT. *Information and Computer Security*, *28*(3), 359–371.

Fornell, C. and Cha, J. 1994. Partial least squares. In Advanced Methods of Marketing Research, Bagozzi, R.P. (ed.), pp. 154-178. Cambridge: Blackwell.

Giwah, A. D., Wang, L., Levy, Y., & Hur, I. (2020). Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory. *Journal of Intellectual Capital*, *21*(2), 215–233.

Gouthier, M. H. J., Nennstiel, C., Kern, N., & Wendel, L. (2022). The more the better? Data disclosure between the conflicting priorities of privacy concerns, information sensitivity and personalization in e-commerce. *Journal of Business Research*, *148*(May), 174–189.

Gregory, R. (2003). Psychological Testing History, Principles and Applications. In *Boston: Pearson Education*.

Handoyo, S. (2024). Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. *Heliyon*, *10*(8).

Hair, J., Ringle, C. and Sarstedt, M.. (2011). Indeed a Silver Bullet. Journal of Marketing Theory and Practice, 19, 139-15

Hair Jr., J.F., *et al*. (2014). Partial Least Squares Structural Equation Modeling (PLSSEM): An Emerging Tool in Business Research. European Business Review, 26,106-121.

Hair, J. F., Ringle, C. M., Hult, G. T. M., & Sarstedt, M. (2016). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (2nd Editio). Sage Publications, Inc.

Hudson, S., & Liu, Y. (2021). Mobile app users ' privacy concerns : different heuristics for privacy assurance statements in the EU and China. *Information Technology*, *36*(1), 245–262.

Henseler, J., Ringle, C. M., & Sarstedt, M. 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43 (1): 115-135.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS quarterly*, 275-298.

Hsieh, J., & Li, H. (2022). *Exploring the fit between mobile application service and application privacy*. *2*(November 2021), 264–282.

Jaspers, E. D. T., & Pearson, E. (2022). Consumers ' acceptance of domestic Internet-of-Things : The role of trust and privacy concerns. *Journal of Business Research*, *142*(December 2021), 255–265.

Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, *107*(August 2019), 106260.

Kang, J.-W., & Namkung, Y. (2019). The role of personalization on continuance intention in food service mobile apps. *International Journal of Contemporary Hospitality Management*, *31*(2), 734–752.

Kaushik, K., Kumar Jain, N., & Kumar Singh, A. (2018). Antecedents and outcomes of information privacy concerns: Role of subjective norm and social presence. *Electronic Commerce Research and Applications*, *32*(September), 57–68.

Keith, M. J., Babb, J., Furner, C., Abdullat, A., Lowry, P. B., Keith, M. J., Abdullat, C., & Lowry, &. (2016). Limited Information and Quick Decisions: Consumer Privacy Calculus for Mobile Applications. *AIS Transactions on Human-Computer Interaction*, *8*(3), 88–130.

Keith, M. J., Lowry, P. B., Babb, J., Lowry, P. B., Furner, C. P., & Abdullat, A. (2016). Limited information and quick decisions: Consumer privacy calculus for mobile applications. *AIS Transactions on Human-Computer Interaction*, *8*(3), 88–130.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human Computer Studies*, *71*(12), 1163–1173.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration (ijec)*, *11*(4), 1-10.

Kolotylo-Kulkarni, M., Xia, W., & Dhillon, G. (2021). Information disclosure in e-commerce: A systematic review and agenda for future research. *Journal of Business Research*, *126*(November 2020), 221–238.

Koohikamali, M., French, A. M., & Kim, D. J. (2019). An investigation of a dynamic model of privacy trade-off in use of mobile social network applications: A longitudinal perspective. *Decision Support Systems*, *119*(February), 46–59.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture intercultural dynamics of privacy calculus. *Business and Information Systems Engineering*, *4*(3), 127–135.

Krosnick, J. A., & Presser, S. (2009). Question and Questionnaire Design. In *Handbook of Survey Research (2nd Edition)*.

Ku, E. C. S., & Chen, C. Der. (2013). Fitting facilities to self-service technology usage: Evidence from kiosks in Taiwan airport. *Journal of Air Transport Management*, *32*, 87–94.

Likert, R. 1932. A technique for the measurement of attitudes. Archives of Psychology, 140: 5-55.

Li, P., Cho, H., & Goh, Z. H. (2019). Unpacking the process of privacy management and self-disclosure from the perspectives of regulatory focus and privacy calculus. *Telematics and Informatics*, *41*(January), 114–125.

Lin, Z., & Filieri, R. (2015). Airline passengers' continuance intention towards online check-in services: The role of personal innovativeness and subjective knowledge. *Transportation Research Part E: Logistics and Transportation Review*, *81*, 158–168.

MacKenzie, S. B., & Podsakoff, P. M. (2012). Common method bias in marketing: Causes, mechanisms, and procedural remedies. *Journal of retailing*, *88*(4), 542-555.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users ' The Information the Scale , and a Causal (IUIPC): *Informs*, *15*(4), 336–355.

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32–44.

Min, H., Park, J. and Kim, H. J. (2016). Common method bias in hospitality research: a critical review of literature and an empirical study. International Journal of Hospitality Management, 56 (July 2016): 126-135.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375.

Mohammed, Z. (2017). *The Role of Cognitive Disposition in Re-examining the Privacy Paradox : A Neuroscience Study by A dissertation submitted in partial fulfillment of the requirements for the degree of*.

Momenzadeh, B., Gopavaram, S., Das, S., & Camp, L. J. (2021). Bayesian evaluation of privacy-preserving risk communication for user android app preferences. *Information and Computer Security*, *29*(4), 680–693.

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, *37*(1), 101413.

Nunnally, J. C., & Bernstein., I. H. (1994). Psychometric theory. 3rd ed. In *New York: McGraw-Hill.*

Offor, P. I. (2016). *Examining Consumers' Selective Information Privacy Disclosure Behaviors in an Organization's Secure e-Commerce Systems* (Doctoral dissertation, Nova Southeastern University).

Olukoya, O., Mackenzie, L., & Omoronyia, I. (2020). Computers & Security Security-oriented view of app behaviour using textual descriptions and user-granted permission requests. *Computers & Security*, *89*, 101685.

Ozdemir, Z. D., Jeff Smith, H., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, *26*(6), 642–660.

Ozturk, A. B., Nusair, K., Okumus, F., & Singh, D. (2017). Understanding mobile hotel booking loyalty: an integration of privacy calculus theory and trust-risk framework. *Information Systems Frontiers*, *19*(4), 753–767.

Polykalas, S. E., & Prezerakos, G. N. (2019). When the mobile app is free, the product is your personal data. *Digital Policy, Regulation and Governance* , *21*(2), 89–101.

Ramayah, T., Cheah, J., Chuah, F., Ting, H. and Memon, M. A. 2018. Partial least squares structural equation modelling (PLS-SEM) using SmartPLS 3.0: An updated and practical guide to statistical analysis (2nd edition). Kuala Lumpur: Pearson.

Rocha, T., Souto, E., & El-Khatib, K. (2020). Functionality-based mobile application recommendation system with security and privacy awareness. *Computers and Security*, *97*, 101972.

Saxborn, M., Pan, Y., & Said, A. (2024, March). Trust Through Recommendation in E-commerce. In *Proceedings of the 2024 Conference on Human Information Interaction and Retrieval* (pp. 87-96).

Shih, D. H., Hsu, S. F., Yen, D. C., & Lin, C. C. (2012). Exploring the Individual's Behavior on Self-Disclosure Online. *International Journal of Human-Computer Interaction*, *28*(10), 627–645.

Škrinjarić, B., Budak, J., & Žokalj, M. (2018). The Effect of Personality Traits on Online Privacy Concern. *Ekonomski Pregled*, *69*(2), 106–130.

Slyke, C. Van, Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for Information Privacy and Online Consumer Purchasing. *Journal of the Association for Information Systems*, *7*(6), 415–444.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989–1015.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring individuals' Concerns About Organizational Practices. *MIS Quarterly*, *20*(2), 167–196.

Soumelidou, A., & Tsohou, A. (2020). Effects of privacy policy visualization on users' information privacy awareness level: The case of Instagram. *Information Technology and People*, *33*(2), 502–534.

Sullivan, G. M., & Feinn, R. (2012). Using effect size—or why the P value is not enough. *Journal of graduate medical education*, *4*(3), 279-282.

Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, *52*, 278–292.

Tay, S. W., Teh, P. S., & Payne, S. J. (2021). Reasoning about privacy in mobile application install decisions: Risk perception and framing. *International Journal of Human Computer Studies*, *145*(October 2019), 102517.

Taherdoost, H. (2019). What is the best response scale for survey and questionnaire design; review of different lengths of rating scale/attitude scale/Likert scale. *Hamed Taherdoost*, 1-10.

Tronnier, F., Harborth, D., & Hamm, P. (2022). Investigating privacy concerns and trust in the digital Euro in Germany. *Electronic Commerce Research and Applications*, *53*, 101158.

Tseng, H. T., Nadeem, W., Hajli, M. S., Featherman, M., & Hajli, N. (2023). Understanding consumers' interest in social commerce: the role of privacy, trust and security. *Information Technology and People*.

Veltri, G. A., & Ivchenko, A. (2017). The impact of different forms of cognitive scarcity on online privacy disclosure. *Computers in Human Behavior*, *73*, 238–246.

Walter, J., & Abendroth, B. (2020). On the role of informational privacy in connected vehicles: A privacy-aware acceptance modelling approach for connected vehicular services. *Telematics and Informatics*, *49*(December 2019), 101361.

Wang, L., Hu, H. H., Yan, J., & Mei, M. Q. (2020). Privacy calculus or heuristic cues? The dual process of privacy decision making on Chinese social media. *Journal of Enterprise Information Management*, *33*(2), 353–380.

Wang, L., Sun, Z., Dai, X., Zhang, Y., & Hu, H. hua. (2019). Retaining users after privacy invasions: The roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. *Information Technology and People*, *32*(6), 1679–1703.

Wang, R., Wang, Z., Tang, B., Zhao, L., & Wang, L. (2020). SmartPI: Understanding Permission Implications of Android Apps from User Reviews. *IEEE Transactions on Mobile Computing*, *19*(12), 2933–2945.

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.

Warner, M., & Wang, V. (2019). Self-censorship in social networking sites (SNSs) – privacy concerns, privacy awareness, perceived vulnerability and information management. *Journal of Information, Communication and Ethics in Society*, *17*(4), 375–394.

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, *106*, 44–52.

Wirth, J., Maier, C., & Laumer, S. (2018). The influence of resignation on the privacy calculus in the context of social networking sites: an empirical analysis.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view.

Yang, Q., Gong, X., Zhang, K. Z. K., Liu, H., & Lee, M. K. O. (2020). Self-disclosure in mobile payment applications: Common and differential effects of personal and proxy control enhancing mechanisms. *International Journal of Information Management*, *52*(December 2019), 102065.

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting User Concerns about Online Privacy. *Journal of the American Society for Information Science and Technology*, *58*(5), 710–722.

Yeh, C. H., Wang, Y. S., Lin, S. J., Tseng, T. H., Lin, H. H., Shih, Y. W., & Lai, Y. H. (2018). What drives internet users' willingness to provide personal information? *Online Information Review*, *42*(6), 923–939.

Zaini, S. M., Noor, N. H. M., & Zandi, G. (2024). The behaviour of e-commerce users: An empirical investigation of online shopping. *Journal of Management World*, *2024*(2), 50-60.

Zhang, R., Chen, J. Q., Lee, C. J., Zhang, R., & Chen, J. I. M. Q. (2016). Mobile Commerce and Consumer Privacy Concerns. *Journal of Computer Information Systems*, *4417*(May), 31–38.

Zhou, T. (2020). The effect of information privacy concern on users' social shopping intention. *Online Information Review*, *44*(5), 1119–1133.