

Article

Privacy Concerns in Social Commerce: The Impact of Gender

Ibrahim Mutambik ^{1,*} , John Lee ² , Abdullah Almuqrin ¹, Justin Zuopeng Zhang ³ , Mohammed Baihan ⁴ and Abdulrhman Alkhanifer ⁵

¹ Department of Information Science, College of Humanities and Social Sciences, King Saud University, Riyadh P.O. Box 11451, Saudi Arabia

² School of Informatics, The University of Edinburgh, 10 Crichton St., Edinburgh EH8 9AB, UK; john.lee@ed.ac.uk

³ Department of Management, Coggin College of Business, University of North Florida, 1 UNF DRIVE, Building 42, Jacksonville, FL 32224, USA

⁴ Department of Computer Science, Community College, King Saud University, Riyadh P.O. Box 11451, Saudi Arabia

⁵ Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh P.O. Box 11451, Saudi Arabia; akhnaifer@ksu.edu.sa

* Correspondence: imutambik@ksu.edu.sa

Abstract: Today, social commerce is one of the most rapidly growing subsectors of e-commerce, creating new opportunities for brands of all types and sizes. However, despite its popularity and potential, social commerce faces significant challenges, including issues of privacy, trust and ethics. This paper sets out to identify key aspects of privacy which influence ongoing user engagement with social commerce, so that social media, and other social commerce, platforms can more effectively address the issue. In particular, the paper seeks to determine the extent to which these aspects of privacy are a function of gender and, therefore, to increase our understanding of the role of gender in determining a user's likelihood of sustainable engagement with s-commerce. To explore these issues, the study deploys a mixed methodology (semi-structured interviews and questionnaires) to examine the views of a broad demographic of s-commerce users in Saudi Arabia. The results allowed us to identify three distinct aspects of online privacy that significantly influence the likelihood of engaging in s-commerce and also demonstrated that the relative importance of these aspects is a function of gender. The study enhances current understanding of the role of gender in intention to use s-commerce and provides a framework for further research. The findings of the study will be of interest to all parties involved in the design and provision of s-commerce services, including social media platforms.

Keywords: social commerce; social media; privacy concerns; sustainable behaviour; gender



Citation: Mutambik, I.; Lee, J.; Almuqrin, A.; Zhang, J.Z.; Baihan, M.; Alkhanifer, A. Privacy Concerns in Social Commerce: The Impact of Gender. *Sustainability* **2023**, *15*, 12771. <https://doi.org/10.3390/su151712771>

Academic Editors: De-Chih Lee and Chih-Chien Wang

Received: 11 July 2023

Revised: 15 August 2023

Accepted: 21 August 2023

Published: 23 August 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Over the past few years, social commerce (s-commerce) has grown rapidly [1]. This is a result of a number of key drivers, such as the increasing ability to take advantage of deals, discounts and exclusive offers [2] and relatively high levels of social support from a peer network [3]. However, another key driver of s-commerce, and one that is growing in importance, is ease of purchase. In a 2022 worldwide Statista survey on factors driving use of social commerce [4], 32% of respondents named “ease of purchase” as an important factor in participation in s-commerce. This suggests that the value of the s-commerce market has the potential to grow significantly more as the use of mobile devices increases, allowing “anytime-anywhere” access to social media for an ever-growing number of people. Social media use is substantially driven by the use of mobile devices [5,6], and social commerce will offer far greater ease of purchase when provided on mobile devices [7,8]. To illustrate this, the number of mobile devices in use globally is predicted by Statista to rise from 4.2 billion in 2020 to 18.22 billion by 2025 [9].

Despite the many factors which positively affect participation in s-commerce, there are also some factors which can, and do, significantly hinder the use of s-commerce. These include the risk of purchasing products of poor quality or illegal products, as well as the risk of financial loss or theft [10,11]. However, one of the main, and enduring, issues that negatively affects the use of s-commerce is concerns over privacy and the security of personal information. Many users fear that the use of s-commerce can expose their personal information to dangers such as unauthorised access or misuse by cybercriminals [12]. These conclusions are supported by studies such as [13,14] (including a recent large-scale meta-analysis by Zerbini et al. [13], although this suggests a more nuanced picture across e-commerce generally), which indicate that concerns about privacy decrease purchase intention in s-commerce. There are also several studies which have examined the effects of privacy concerns on engagement with the Internet in general, and all report that the issue is a significant challenge for all online platforms and organisations [15–19].

Most social media platforms are aware of the privacy concerns of potential s-commerce users and have taken steps to mitigate them through the use of privacy policies and by giving users features that offer a perception of some degree of control over their private information. This has had some effect, and research has shown that privacy assurance has a positive influence on trust, which ultimately increases the likelihood of purchase on s-commerce sites [20]. Despite this, however, many social media users are hesitant about engaging with m- or s-commerce, due to the possibility that their personal information could be shared with other third parties, both legitimate and illegitimate, without their consent [15,16]. Identity theft is another significant concern of users [21]. The extent to which these threats are real is not a determining factor in the context of s-commerce behaviour: it is the perception that has an impact on intention to use and consequent behaviours. However, there are obvious ethical issues if purchasing behaviour is induced or encouraged, which is actually risky or unsafe given the reality of the threats. Ideally, real threats will be minimised, and users will be well informed so that their perceptions, and hence behaviour, are appropriate to the real threat level. Growth in s-commerce needs to be not only sustainable, but also responsible.

While there is considerable research that seeks to understand the attitudes of Internet users towards privacy in general, and some which looks at privacy in the context of s-commerce, there are relatively few studies which specifically aim to examine gender differences in attitudes towards privacy. Gender can be an important parameter for s-commerce providers, because markets are often strongly differentiated by gender [8], e.g., in areas such as fashion, technology, housewares, etc. Moreover, social media user groups are strongly differentiated by gender [5].

Some studies have found real attitudinal differences between men and women, in terms of privacy, but these studies tend to be focused on the behaviours of specific demographic groups, such as teenagers or students [22], on a single and specific social media platform [23], outside of the context of s-commerce. It has also been found that, in a general online context, women tend to be more concerned about privacy compared to men [24]. Although not specifically designed to examine how gender differences in privacy concerns impact on s-commerce, it is interesting to note that one study has found women to be more inclined than men to share certain kinds of less sensitive private information on social media in exchange for customer benefits [25,26]. This may have relevance in an s-commerce environment.

This study sets out to add to the current knowledge by examining the impact of gender differences in privacy attitudes on intention to engage with s-commerce. The paper focuses specifically on seeking insights relating to two main questions:

RQ1: Do differences in attitude towards online privacy, between men and women, in Saudi Arabia, impact the intention to use s-commerce?

RQ2: To what extent do these differences, if they exist, impact reported behaviour, in terms of engaging with s-commerce?

An examination of the impact of gender on attitudes towards online privacy, and the consequent use of s-commerce, will contribute to current knowledge, act as the basis for further research and provide a guideline for s-commerce platforms, regulatory authorities and other relevant bodies, for designing policy. This will be useful for commercial reasons, as well as political and cultural reasons in regions where different gender roles apply.

2. Literature Review

In the context of this study, there are three main areas of interest within the literature.

2.1. Social Commerce

The term social commerce (s-commerce) is essentially a portmanteau phrase derived from combining social networking and e-commerce and is a “form of commerce mediated by social media” [27]. Allowing users to buy and sell goods and services within a social media platform, it is a model which extends the role of social media, by encouraging users to carry out the purchase process without leaving the app. This, according to McKinsey [28] removes friction from the purchasing process, produces a more engaging consumer journey, and presents new opportunities for brands to increase consumer awareness.

S-commerce is often predicted to be an area of large potential growth. This is principally because, in 2021, almost half of the world’s population (some 3.5 billion people) were using social media, and the number continues to grow rapidly, while consumers spend, on average, two hours a day on social platforms [29]. However, although the use of s-commerce is expanding quickly, the drivers of this growth are not fully understood. Some studies have shown a clear association between the intention to use s-commerce and utilitarian benefits such as cost-savings and convenience, while others have suggested that emotional factors, such as pleasure, are important [11,30]. Other recent studies have identified environmental issues, such as sustainability, as having an impact on user behaviours in an s-commerce context, while others have established a positive connection between purchasing intention and WOM (word-of-mouth) recommendations [29]. One of the most significant factors in influencing user intent and behaviour, however, is the issue of privacy.

2.2. S-Commerce and Privacy

Online, or digital, privacy can be defined as an individual’s right to be protected from unauthorised sharing of the personal information provided to a website or platform and the individual’s right to be protected from unauthorised publicity, examination, usage, or monitoring of their digital information or activities [31,32]. Providing such protection is a real and growing problem, especially in a big-data economy, where cybercrime is increasingly common and where machine learning algorithms are designed to recognise and commercially exploit patterns, trends and behaviours exhibited by users [33,34]. The result is that concerns over privacy are growing. This is perhaps understandable in the light of data breach statistics over the past few years (where, even if there is improvement in some areas [31,32], the picture in the Middle East is concerning [7,8,35]). Yet, s-commerce also continues to grow. This might be seen as a manifestation of the well-known “privacy paradox” [36], whereby users of online services are concerned about privacy risks but persist in taking little or no action to reduce them.

An important contributor here is the fact that users often do not fully understand the risks involved with using an application or platform. Although most social media (and other online) platforms do take some measures to protect users and publish privacy policies to explain users’ rights and responsibilities, these policies are often long, complex and legally worded documents which are designed to protect the provider rather than the user [33,37]. On many occasions, users simply do not engage with the relevant policies, but even if they did, it is questionable whether this would help them to appreciate the risks, because policies tend to describe, for example, how information will or may be shared, without describing the risks as such. In the end, the risks arise from complex social factors that extend far beyond a given s-commerce context, influencing the behaviour

of s-commerce providers and many other organisations and individuals. Mitigation of the risks is often more a consequence of legal and regulatory frameworks than anything else [38]. In the long run, the sustainability of s-commerce (or e-commerce generally) will depend on equitable and responsible approaches emerging to these wider social issues.

While the benefits, to both buyers and sellers, of s-commerce are widely recognised, and despite the fact that risks may be ill-understood, the restraining effect of users' privacy concerns on the sustainable growth of the market is also well documented. In fact, the impact of privacy concerns on the broader market of e-commerce has been recognised for over two decades [39,40]. More recent research has shown that these concerns still exist. A study by Fortes and Rita [40], for example, found that privacy concerns when online have a negative impact on several factors which influence intention to purchase, including trust, perceived usefulness, perceived ease of use and perceived behavioural control. It is natural to presuppose that these concerns about the general e-commerce environment will migrate, at least to some extent, to the s-commerce environment, and this expectation is supported by research [41,42].

The fact that individuals vary widely in their attitudes, and in their consequent behaviour, towards privacy is well known. Often, these variations are a result of external factors such as culture [43,44], but they can also result from internal psychological or personality traits [32,45]. This leads to the question of the quantification of privacy concerns—how, in other words, can privacy concerns be effectively measured?

Several methodologies have been proposed for the purpose of measuring an individual's privacy concerns. Earlier approaches, however, were based on single-dimensional models which provide only a broad-brush picture which lacked depth and detail [46,47]. Subsequently, other tools, based on a multi-dimensional approach, have emerged, and these have proved more informative in terms of understanding an individual's concern for privacy. The first tool of this kind, developed by Smith, Milburg and Burke in 1996 [48], identified four factors—errors, collection, secondary use and unauthorised access to information—as the dimensions of privacy concern and became known as the Concern for Information Privacy (CFIP) scale. Although the CFIP was a significant step forward, the model was further developed by Malhotra, Kim and Agarwal in 2004, who introduced a multidimensional notion of Internet Users Information Privacy Concerns (IUIPC) [49]. This model has since become one of the most endorsed scales of privacy concern [49] and provides a reliable and valid measurement tool which has been used in many studies related to Internet use [46,47].

2.3. Gender and Attitudes to Privacy

This research on an individual's attitude to privacy prompts the natural question of whether attitudes differ between the sexes, and—if so—how, and to what extent. Interest in this question has grown steadily over time, and there has been a considerable number of studies which have sought to provide insights. Some studies of gender differences (in privacy attitudes) in a general (offline) context have suggested that women tend to have a greater perception of risk and lower risk behaviours than men [19], which might go some way to accounting for why women are more concerned about their privacy and less likely to share personal information than men [19,24]. These results have been reflected by studies in an online context. Studies such as those by Fogel and Nehmad [50] and Hoy and Milne [23] showed that women are, in general, more concerned with their privacy than men, while other research has shown that, in an online setting, women are less likely to share specific personal details such as phone numbers than men [51]. Behavioural differences in sharing personal information (online) are critical as unless stringent steps are taken to protect it, such data can easily be shared and abused without the user's consent [8,52]. Despite these greater inhibitions, it has been found that women spend more time than men using social media [24,26] and, as noted above, that they are more predisposed to share certain kinds of personal information if a reward is involved [26].

While these studies have made significant contributions to our understanding of the relationship between gender and privacy, most refer to a general context; relatively few relate specifically to the s-commerce environment. This is the focus of the current study. It is also worth noting that there is little existing evidence for the contention that gender is a strong determinant of concerns over online privacy. In one 2022 study, for example, which sought to establish a methodology for predicting “privacy personas”, it was found that age was the most significant factor in privacy concerns, while gender and education were poor predictors of an individual’s profile for privacy concerns [53].

3. Research Method

To ensure the validity and reliability of the data [54,55], the current study uses a two-stage method approach: qualitative and quantitative. The first (qualitative) of these methods collects data from semi-structured interviews, while the second (quantitative) method collects data from questionnaires. These stages are described in more detail in Sections 4 and 5.

The study followed, at all stages, standard ethical guidelines provided by King Saud University’s Research Ethics Committee (KSU-HE-12-242). All participants were assured (in writing) of confidentiality and advised as to the purpose of the study and how data would be used. All data were collected with full participant consent, and they were advised that they could withdraw from the study at any time. All data, from all sources, were fully anonymised. Participation was completely voluntary, and no financial (or other) incentive was offered to any participant.

4. Exploratory Stage

This stage uses semi-structured interviews to gain insights into the various factors which influence an individual’s attitude towards online privacy, and how (if at all) these factors affect engagement with s-commerce. An analysis (thematic) of these interviews was combined with an analysis of existing literature, and the findings of other research, to build the research model of the study and formulate hypotheses.

4.1. Sample and Data Collection Procedure

The data collection procedure used interviews with 20 randomly selected professionals with varying degrees (a minimum of one year) of experience in using social media and s-commerce. Participants were selected from diverse professional backgrounds, and an approximately equal mix of genders (male/female) was used. The sample size was determined using the principle of saturation [56]. The sample size of 20 was considered enough to provide meaningful results, as, after this point (17 interviews), participants supplied no new information, perspectives or ideas. Each interview lasted about an hour and followed a similar format. Each interview was also taped for transcription and analysed at a later stage. Interviews were conducted and analysed in Arabic and translated into English only for purposes of presentation in this report. Further details about the interviewees are shown in Table 1 below.

Table 1. Summary of participant profiles.

Participant Profiles		Frequency
Gender	Male	10
	Female	10
Social commerce experience	<3 years	5
	3 to 5	11
	6 to 10 years	4
Professional background	Humanities	14
	Sciences	6

4.2. Findings of the Exploratory Stage and Hypothesis Development

Thematic analysis was used to analyse the text content of the interviews. This resulted in the identification of three distinct domains of (information) privacy that have a significant effect on the readiness of those using social media platforms to engage in s-commerce. These aspects are the following: Awareness and Acceptance of Privacy Policy (AAPP), Collection and Use of Personal Information (CUPI) and Perceived Control of Private Information (PCPI). These factors are defined as follows:

AAPP—a measure of users' belief in the relevance and effectiveness of privacy policies (specific to the platform) in protecting and safeguarding private data.

CUPI—a measure of the level of user concern that the service provider will abuse private data.

PCPI—a measure of a user's confidence that they are in control of any private information provided to the service provider.

The extent to which these factors were found to vary with gender and how they impact the user's readiness to engage with s-commerce is discussed in the following sections. Figure 1 below shows the research model. This proposes a relationship between PCPI, AAPP and CUPI, and how these factors influence a user's decision to engage with s-commerce, which is based on the theory of reasoned action (TRA) [57].

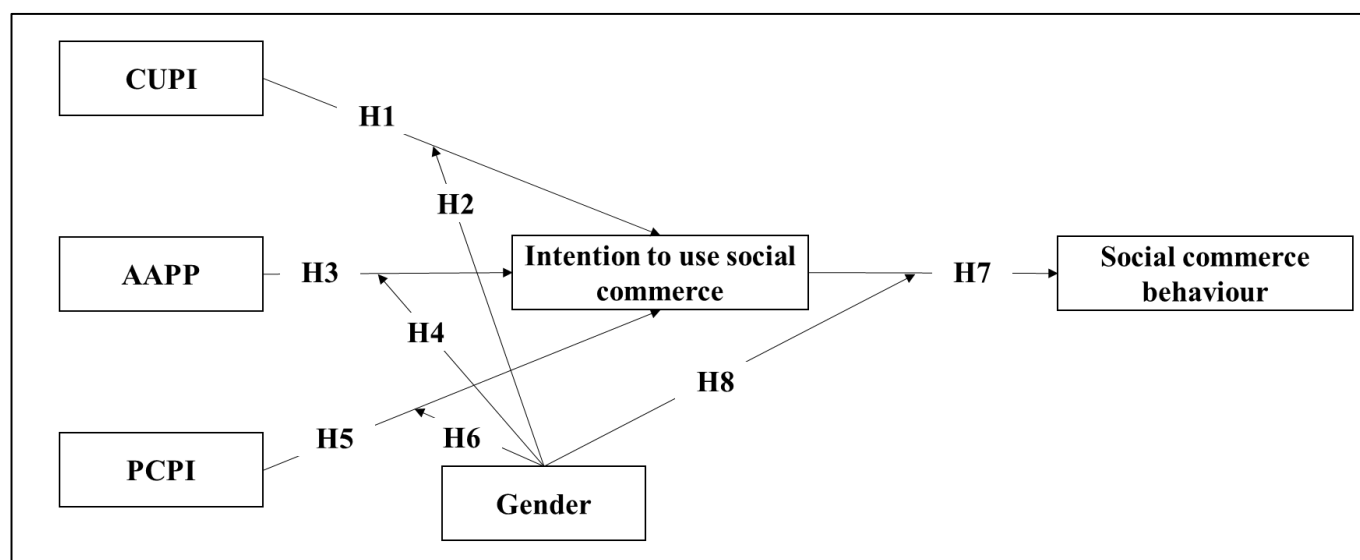


Figure 1. Research model.

4.2.1. Collection and Use of Personal Information (CUPI)

Concerns over how service providers might use or abuse private information significantly affected both the male and female elements of the sample. However, there were also clear differences in the nature of these concerns and the level to which they affect readiness to engage with s-commerce. Overall, men tended to take a more pragmatic view of the situation and displayed a higher risk profile. One male participant commented, for example:

Most things in life involve a risk reward equation. The same is true with s-commerce. In order to take advantage of s-commerce, you have to share some private information, but the risks of this being abused are relatively small compared with the rewards on offer.

Another participant expressed a similar view:

This is a highly connected, digital world which can offer many benefits. The cost is that you have to make some private information publicly available in order to engage with it. It's true that this information could be abused, but it's a risk we have to take. Having said

that, it's always worth looking at the privacy policies of the app you are using, to check that the risks are minimised.

These comments reflected the general male position that sharing private information is an inescapable part of implementing services such as s-commerce, and that while service providers should take appropriate steps to protect that information, there is also an onus on individuals who want to participate in such services to take an interest in the process of safeguarding data. These views contrasted quite markedly with the attitudes of female participants, which often reflected a condition of uncertainty, if not fear. One such participant commented, for example:

The amount of information you need to supply seems totally unnecessary for the services provided. What's worse is that once you've given up this information, you usually have no control over it, and it could be abused in lots of ways. And what does one do when there is a misuse of one's data? I find the whole situation very worrying.

Another participant remarked:

Stories of how private information has been abused are all around us. It's scary. Although I do quite a lot of s-commerce, it took me quite a while to gain the confidence to do so, and—even now—I'm forever worrying about what could happen if my private information falls into the wrong hands.

This feeling of powerlessness was expressed by another female participant:

The problem is that you have very little say over how your information is used. The privacy policies they publish are usually impenetrable legal jargon, so you have no idea whether you're protected or not—and if your data is abused what action can you take? These social media companies normally hold all the power.

Overall, the position of female participants was one of general scepticism, together with serious concern over how privacy issues are handled by social media and s-commerce providers. While the male participants also had concerns, they tended to have a more practical and optimistic outlook which was less likely to stand in the way of engaging with s-commerce. Despite this difference in risk perception, however, there was a general understanding among all participants that information abuse is always possible, and that the problem needs to be addressed by service providers for s-commerce to be successful.

This is a general position that reflects the findings of existing literature. Perceptions of data collection and use are one of the most important factors affecting online activity [58–60], and—whatever an individual's gender—they can significantly affect a person's decision to use a site or its services [61]. It has also been demonstrated that privacy concerns affect people's trust in service providers of all kinds, including s-commerce [62]. However, it has also been noted that trust is a “repairable” concept, providing that appropriate actions are taken by service providers after any invasion of privacy [62]. Based on these findings from the exploratory study and literature review, we hypothesise that:

Hypothesis 1 (H1). *CUPI has a significant impact on users' intention to share private information for the purpose of engaging in s-commerce.*

Hypothesis 2 (H2). *If hypothesis H1 is supported, then the degree of support varies with gender (male/ and female).*

4.2.2. Awareness and Acceptance of Privacy Policy (AAPP)

There are a number of studies which show that users' awareness [63–65] and engagement with privacy policies strongly influences readiness to use s-commerce [63,64]. It is also true that low awareness of privacy policies increases willingness to share private data [64,65].

However, the extent to which gender plays a role in determining the relationship between policy awareness and intention to use s-commerce is not clear from the existing

literature. The results from this study suggest that women are more cautious about sharing personal information, which aligns with the suggestion of the CUPPI theme that men have a higher risk profile. One male participant, for example, said:

I'm aware that all the big platforms publish extensive privacy policies, but, to be honest, I rarely engage with such policies these days. They're usually written to cover the service providers back, not the users, and it's often difficult to make sense of them.

Another male participant made a similar remark:

The length and technical nature of a typical privacy policy makes them pretty well inaccessible to most users. I think that this is probably true with all online platforms, not just social media and s-commerce.

This scepticism was echoed by other users. For example:

I know I should read them, but I don't actually do so very often. As far as I can tell, they are a cut and paste exercise from other companies, so when you've read one you've read them all. However, it worries me if a service provider doesn't actually have a privacy policy.

While these sentiments were broadly shared by the female participants, they (female participants) seemed to be more willing to engage with privacy policies. One (female) participant said of privacy policies, for example:

They're usually hard to understand, and they're long and tedious, but it's worth making the effort to read them, to make sure that your private stuff is protected at least to some degree. Everyone knows what can happen if your private information gets into the wrong hands.

Another female participant commented:

Privacy policies are important, but in my experience they tend to be very generic and usually built to fit the laws of Western countries, so don't take account of regional cultural or religious needs. All the same, I do always scan the relevant policy before signing up to a platform or app, especially in s-commerce, which can expose you to more risk than some other activities.

This impulse among female users to read policies despite viewing them cynically was displayed in several comments. For example:

I like to know where I stand when it comes to privacy and sharing information, so I nearly always have a brief look at the privacy policy. I wouldn't be very confident that these policies actually prevent abuse, though. The big companies know that most users either don't understand them, or are too involved in their [s-commerce] activities to care.

In terms of general online activity, the existing literature provides conflicting conclusions on the relationship between gender and information privacy [66]. Some studies have found that the perception of strong privacy practices has a greater effect on women [24,63,67], but others have shown that men are more strongly affected [64,65]. Other research has concluded that there are no differences between genders [68]. Although the current research is not conclusive, it strongly suggests that there are real and significant differences between the genders when it comes to the impact of awareness of privacy policy on the use of s-commerce. We therefore propose the following hypotheses:

Hypothesis 3 (H3). *AAPP has a significant impact on users' intention to share private information for the purpose of engaging in s-commerce.*

Hypothesis 4 (H4). *If hypothesis H3 is supported, then the degree of support varies with gender (male and female).*

4.2.3. Perceived Control of Private Information (PCPI)

Engagement in s-commerce is strongly related to users' belief that they are in control of their personal data. Further, the literature suggests the perception of control is an important factor in determining information-sharing behaviour. This seems reasonable at an intuitive level and is borne out by the evidence, as perceived control of information plays an active role in internet information-sharing behaviours [69–71]. Further, users of social media platforms such as Facebook and Twitter share information with the sites depending on perceived level of control over its use [72,73].

Overall, the current research supported all of these findings, suggesting that PCPI does have significant influence on information sharing for s-commerce purposes. Compared with the other two themes, the gender divide in this theme was relatively small and subtle. Despite this, such a divide does exist. For example, the perspective of male participants was represented by the following comments from male participants:

As users usually have little or no control over what happens to the data they share, then that information is vulnerable to abuse. This means that users should only share the minimum amount of information that's required by the platform, in order to mitigate risks.

Given that you can't control what happens to the information that you supply, it makes sense to share it only if you have to. I tend to feel more confident about platforms that give the user some level of ability to edit and control private account information through a settings panel—the implication is that these platforms care more about data security and privacy than platforms which don't give this facility.

These comments suggest that male participants may feel that the issue of PCPI is principally the responsibility of the individual, and that any sense of vulnerability and/or lack of control could be reduced significantly by moderating the private information supplied to the (s-commerce) platform.

However, while the female participants shared this view to a certain extent, they differed in the mechanisms by which an individual fulfils this responsibility. For instance, one female participant said:

Most s-commerce platforms allow users some control over the amount of information they provide, but they often give very little guidance or advice on how to use things like filters and passwords effectively. This leaves many users thinking they have less control than they really do.

As with the male participants, this seems to put the onus of responsibility onto the individual, but for slightly different reasons. It implies that users could mitigate their vulnerability to data abuse by learning how to better manage and protect their personal information. This view was echoed by another participant:

There's not much point in expecting governments or tech companies to provide high levels of data protection, so users need to become more tech savvy.

Based on the findings from the exploratory study and the literature reviewed in relation to this theme, it is therefore hypothesised that:

Hypothesis 5 (H5). *PCPI has a significant impact on users' intention to share private information for the purpose of engaging in s-commerce.*

Hypothesis 6 (H6). *If hypothesis H5 is supported, then the degree of support varies with gender (male/female).*

4.2.4. The Effect of Attitude and Intention Behaviour

As has been established through the Theory of Reasoned Action [57], intentions are different from behaviours. While an intention to engage in a certain behaviour is a strong predictor of actual behaviour, it does not guarantee that the individual will in fact engage

in that behaviour. This research model was therefore developed around the three thematic areas (CUPI, AAPP and PCPI) in conjunction with the Theory of Reasoned Action (TRA). The model seeks to establish the extent to which intention is linked to behaviour in each of the thematic areas. We thus hypothesise that:

Hypothesis 7 (H7). *The intention to share personal information influences users' information sharing behaviour.*

Hypothesis 8 (H8). *If hypothesis H7 is supported, then the degree of support varies with gender (male/female).*

5. Confirmatory Stage

As noted above, this stage of the study deployed a questionnaire developed from the outcome of the first stage of the research. The questionnaire was used to validate the structure of the research model and to identify any differences in privacy concerns between s-commerce users that could be attributed to gender.

5.1. Developing the Research Questionnaire

There are several ways of developing questionnaires. In this study, we employ a set of 20 questions, based on a 5-point Likert scale, to gain an understanding of how an individual's concerns about information privacy impacts their decision to use s-commerce. Most questions were developed for this particular study, based on the data from the interviews in stage one, though some were derived from existing questions that have been successfully used in previous studies. To identify any problems of clarity to participants, and to ensure that the questions were returning meaningful data, the questionnaire was piloted with a group of 20 s-commerce users, 10 males and 10 females. As a result of the pilot, some minor adjustments were made to questions.

5.2. Content Validity Assessment

As a first step, prior to data collection [74,75], a survey validation exercise was carried out [76,77]. This used several experts, each with significant experience in the research field [78]. Each expert reviewed and assessed each item in the questionnaire [75,78]. A total of 7 experts were invited by email to participate and 6 responded. This is significantly more than the number of external validators required for meaningful feedback, which is generally agreed to be three [79]. Based on the expert assessments of the questionnaire, two questions were removed, resulting in a final survey of 18 fully validated questions. These 18 items were again reviewed to check clarity and consistency, before the primary data collection phase.

5.3. Primary Data Collection

The study used a simple random sampling strategy to connect with a large number of participants. The online survey was hosted by the widely used internet-based application Google Forms, and the data were collected over a period of two months in early 2023. All those invited to participate were known to be social media users based in Saudi Arabia with an interest in s-commerce. Reminder emails were sent to non-responders on a bi-weekly basis. In all, a total of 266 questionnaires were returned, 1 of which was eliminated due to missing information, leaving 265 valid questionnaires. Table 2 summarises the key demographics of the sample. The language used was Arabic, which is translated into English for the purposes of this report.

Table 2. Sample demographics—summary.

Participant Characteristic		Frequency
Gender	Male	133
	Female	132
S-commerce experience	<3 years	90
	3 to 5	99
	6 to 10 years	76
Professional level	Student	77
	Qualified	178
	Retired	10
Age	<25	101
	25–50	141
	>50	23

Ensuring that respondents filled out the questionnaire correctly was an important concern in this research. Following the recommended guidelines by many authors (e.g., Creswell and Clark [80]), several steps were taken to address this issue:

- Respondents were provided with clear and concise instructions about the purpose of the survey and how to complete it—this included information about how to answer each question and how to complete the questionnaire within the given time frame.
- Clear and concise language was used in developing the research questionnaire (see Section 5.1 for more details).
- Respondents were given an option to email or call the researchers to clarify any ambiguous responses or ask additional questions.
- Before administering the questionnaire to the target population, a pilot study was performed (see Section 5.1 for more details).

It is important to note that no method is foolproof, and some respondents may still provide inaccurate or incomplete responses despite researchers' best efforts. However, employing these strategies helped to minimize the risk of errors and increase the validity and reliability of the data collected.

5.4. Descriptive Statistics and Normality Testing

In order to assess the assumption of normality for all factors, the skewness and kurtosis scores were tested. The results, as given in Table 3 below, reveal that the skewness and kurtosis values for all factors were less than the ± 2 cut off value recommended in the literature [81]. This means that the data are normally distributed and appropriate for evaluating the measurement model.

Table 3. Skewness and kurtosis values of factors.

Factors	Kurtosis Statistic (Male–Female)	Skewness Statistic (Male–Female)
Intention	1.358	−1.053
Behaviour	−0.485	−0.351
PUCI	−0.766	−0.253
PCPI	0.679	−0.949
AAPP	1.326	−1.577

5.5. Data Analysis Techniques

Version 21 of the SPSS (Statistical Package for the Social Sciences) was used to code the collected raw data and prepare the data for further analysis. For example, the maximum, minimum and frequency scores of each question were determined to make sure the data were entered accurately. The data were also assessed to identify any potentially missed

data [81]. Structural equation modelling (SEM) was then used to analyse the psychometric properties of the measurement model as well as for hypothesis testing. There is some debate in the literature over the relative merits of covariance-based SEM (CB-SEM) and partial least squares SEM (PLS-SEM) (see, e.g., [74,75,82], among many others). It is sometimes said that they produce very similar results in a variety of circumstances [78,81], but a consensus emerges that CB-SEM is useful with samples that are normally distributed and not too small, whereas PLS-SEM is more flexibly applicable also to smaller and non-normally distributed samples. One of the most authoritative sources, Hair et al. [81], claims that “the PLS-SEM method is much more appropriate at the theory development stage than is CB-SEM” (p. 119). Hence, even though the data are quite normally distributed, as shown above, PLS-SEM is applied in this study, using SmartPLS 4.

5.6. Testing the Measurement Model

Factor loading, Cronbach’s alpha (CA), average variance and composite reliability (CR) were used as measures of the internal consistency, construct validity and reliability of the model [81]. As can be seen in Table 4, each factor loading is over 0.6, and Table 5 shows that the values of CA and CR are greater than 0.7, with AVE greater than 0.5 in each case. This analysis confirms the internal consistency reliability, as well as both discriminant and convergent validity [81,83]. It was also noted that the nature (self-reported) of the questionnaires used in the study could lead to low variable validity, due to common method variance (CMV). It is possible that this could impact the rejection or acceptance of a hypothesis [81,83]. However, the analysis results indicated that CMV was not a significant issue. A potential source of bias arises from the fact that the questionnaire items, as shown in Table 4, tend to request ratings of positive attitudes, with a lack of negative ones for balance. If present, however, this bias should be uniform across the items and participants, and hence not affect the comparisons that are at the heart of the study.

Table 4. Constructs, items with factor loadings and sources.

Constructs	Items	Loading	Source
Intention	I will continue to share information for social commerce purposes.	0.85	[38]
	I intend to continue frequently sharing information for social commerce purposes.	0.86	
	Sharing information for social commerce purposes will continue to be part of my daily activities.	0.87	
Behaviour	I often share information for social commerce purposes.	0.88	[57]
	I am happy to share my experiences of social commerce with other users.	0.89	
	I often share information for social commerce purposes.	0.85	
CUPI	I worry about how social commerce platforms use my personal data.	0.84	Self-developed, based on the qualitative data and [48].
	It frequently concerns me when a social commerce platform demands personal data.	0.84	
	I am against providing personal data to social commerce platforms.	0.83	
	I have concerns that my personal data is passed on to third-parties by social commerce platforms.	0.81	
PCPI	Having control of your own personal data is essential for privacy.	0.84	Self-developed, based on the qualitative data and [59].
	I feel more confident when I can control the information I supply to a social commerce platform.	0.83	
	Privacy settings are important for controlling data provided to a social commerce platform.	0.82	
	I am more likely to take part in social commerce when I can control the use of my personal information supplied to the platform.	0.81	
AAPP	I believe privacy policies reflect a social commerce platform’s commitment to protecting users’ privacy.	0.80	Self-developed, based on the qualitative data and [60].
	I believe that privacy statements mean that my personal information will be properly safeguarded by social commerce platforms.	0.78	
	I feel confident that social commerce platforms genuinely try to comply with their privacy statements.	0.83	
	I believe that privacy policies on social commerce platforms are an important and effective approach to building trust among users.	0.81	

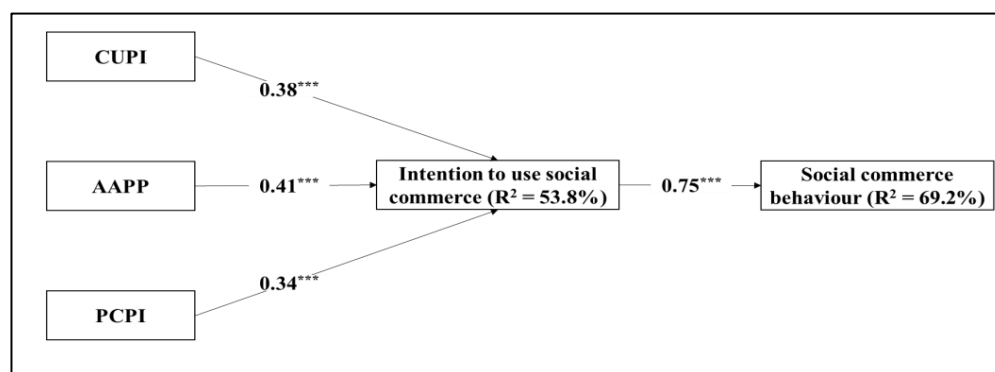
Table 5. Correlations, Cronbach's alpha (CA), composite reliability (CR) and average variance extracted (AVE).

Constructs	CA	CR	AVE	Correlations				
				ISI	IS	CUPI	PCPI	AAPP
Intention	0.87	0.86	0.71	0.84				
Behaviour	0.88	0.84	0.73	0.55	0.85			
PICU	0.85	0.85	0.70	0.63	0.70	0.84		
PIC	0.86	0.81	0.67	0.55	0.65	0.75	0.82	
AEPP	0.88	0.80	0.65	0.52	0.63	0.64	0.57	0.79

Note: Square root of AVE shown in bold as the diagonal.

5.7. Results of Structural Model Evaluation

Structural model analysis evaluation and hypothesis testing was carried out using SmartPLS, and the results are shown in Figure 2. This shows that PCPI, CUPI and AAPP account for 53.8% of the variance in intention to share information and 69.2% of the variance in information sharing behaviour. This means that a significant amount of variance is explained [84]. The results of the research suggest that all of the study's hypotheses are supported. PCPI, CUPI and AAPP were all found to have significant effects on users' attitudes towards information sharing, as well as their intention to share information. This has a consequent effect on information sharing behaviours in an s-commerce context. The *t* values and standardised path coefficients of the model are presented in detail in Table 6.

**Figure 2.** Research model (results of structural model evaluation using the whole sample, *** $p < 0.01$).**Table 6.** Path coefficients and *t* values for full sample.

Hypothesis	Standardised Path Coefficient	T Value	Support?
H1: CUPI has a significant impact on users' intention to share private information for the purpose of engaging in s-commerce.	0.38	5.55 ***	YES
H3: AAPP has a significant impact on users' intention to share private information for the purpose of engaging in s-commerce.	0.41	5.59 ***	YES
H5: PCPI has an impact on users' intention to share private information for the purpose of engaging in s-commerce.	0.34	5.10 ***	YES
H7: The intention to share personal information influences users' information sharing behaviour.	0.75	6.56 ***	YES

Note: ***: 0.001 significance.

Further, the model fit was based on PLS-SEM as shown in Table 7. The fact that the two indices, NFI (normed fit index) and CFI (comparative fit index), are both above the recommended threshold (0.9) suggests that the model was a good fit. Further, the RMSA (Root Mean Square Error of Approximation) was below the recommended threshold of 0.05 [85], again suggesting the acceptability of the model. The chi-square value was 2.21,

which is also less than the recommended threshold of 3.0 [86]. All the model-fit indices exceed the normal acceptance levels, confirming that the measurement model was a good fit with the data collected for this study.

Table 7. Goodness of fit indices.

Fit Index	Results	Recommended Criteria
Absolute fit measures		
Chi-Square (χ^2/DF)	2.21	<3.0
RMSEA	0.043	<0.05
GFI	0.938	>0.90
SRMR	0.939	>0.80
Incremental fit measures		
AGFI	0.931	>0.90
NFI	0.953	>0.90
IFI	0.951	>0.90
CFI	0.976	>0.90
Parsimonious fit measures		
PNFI	0.673	>0.50
PGFI	0.632	>0.50

5.8. Gender Differentials Based on the Model—Analysis of the Model Paths

A multi-group partial least squares (PLS) analysis was used to test the hypotheses concerned with gender differences (male/female). This was achieved through comparison of the corresponding path coefficients in the structural model of both groups using a *t*-test [87]. PLS is also useful for identifying differences among subgroups [88]. The analysis of the sample (male:female = 133:132) showed that the standardised path coefficients were significantly higher for females compared to males ($p < 0.05$), supporting H2, H4, H6 and H8 (see Table 8). Although they are statistically significant, the standardised comparisons between females and males (ranging between 0.14 and 0.17) are small [81].

Table 8. Standardised comparisons of paths between females and males.

Hypothesis	Female (<i>n</i> = 132)		Male (<i>n</i> = 133)		Standardised Comparisons of Paths	Support?
	Standardised Path Coefficient	<i>t</i> -Value	Standardised Path Coefficient	<i>t</i> -Value	Δ Path (Female–Male)	
H2.	0.61 ***	5.58	0.46 **	4.94	0.15	YES
H4.	0.51 ***	5.11	0.37 **	3.21	0.14	YES
H6.	0.62 ***	5.42	0.47 **	4.90	0.15	YES
H8.	0.71 ***	5.72	0.54 ***	5.15	0.17	YES

Note: ***: 0.001 significance, **: 0.01 significance.

6. Discussion

With the constant advancement of technology, it becomes ever easier to capture, store and share information. As a result, it becomes more and more difficult to protect and control personal data while online. In recent years, this has become a critical issue, as the number of people spending a significant amount of time online increases rapidly and as activities such as s-commerce emerge which require individuals to make private data available to host platforms. However, although the protection of online privacy is one of the most important and challenging issues in today's digital world, the majority of studies related to the subject tend, understandably, to focus on the ethical behaviours of companies, individuals and public organisations [16,89,90].

In this study, we are more focused on how concerns over information privacy affect users' attitudes and intentions to engage with online services. In particular, we seek to better understand how privacy concerns impact sustainable engagement with the relatively new activity of s-commerce, and whether this impact varies between genders (male/female). The paper seeks to contribute to the existing gender-based narrative on online information sharing and privacy issues. While there are several studies which examine the relationship between gender, intention and behaviour, there are relatively few that focus on this relationship in the context of s-commerce. The paper is further differentiated from the existing literature in that it uses a two-stage method, consisting of quantitative and qualitative elements, to systematically develop the research model. Carried out in two stages (exploratory and confirmatory), the research provides a more detailed and nuanced understanding of the relationship between gender, privacy concerns and active engagement with s-commerce.

We divide our further discussion into two parts: one focussing on implications for theory and investigation in the academic context, the other on managerial implications.

6.1. Implications for Research and Theory

The research produced a number of outcomes which add to our current knowledge. Most notable of these outcomes is the importance of three specific themes related to information privacy, namely, CUPPI (Collection and Use of Personal Information), PCPI (Perceived Control of Private Information) and AAPP (Awareness and Acceptance of Privacy Policy). The findings of the study showed, for example, that CUPPI strongly influences users' attitude and intention (H1), which, in turn, influences their sustainable behaviours (with respect to s-commerce). This finding reflects the work of other researchers [47,49], who have found that privacy is a primary concern to those who share information for the purposes of engaging in s-commerce.

A similar result was found for PCPI (H5), highlighting the importance of how the control of information is perceived. It has been demonstrated that while users of social media and s-commerce platforms do not have much actual control, greater PCPI has a powerful effect. Other studies have implied the same effect by demonstrating that, in a similar way, greater perceived risks can reduce users' engagement with online platforms [91,92]. This means that strategies such as giving users more settings for the control of their information and ensuring that privacy policies are in place are likely to increase the perception of control and, therefore, levels of engagement. As noted before, there is an important responsibility implied here to ensure that users are not given misleading perceptions and hence drawn into inappropriately risky behaviour.

The study also found that AAPP influences users' intention to engage (H3), in that the greater the level of AAPP of users on an s-commerce platform, the more they are likely to engage. This finding is echoed by some similar studies, such as those by [93,94]. Although there is widespread recognition that, in practice, users rarely read or understand privacy policies, it is crucial that they exist and that users have confidence in them [38].

Possibly the most significant contribution of this paper is that it highlights a potential weakness in the assumption of the existing literature concerning information sharing. This assumption is that the various factors which influence the decision to share information online, and specifically in an s-commerce context, affect males and females to a similar extent [16,95]. This study, however, found that while key factors such as CUPPI, PCPI and AAPP all influence the decision of both males and females to share private information, they do so to different extents. This supports the contention that gender plays a moderating role in an individual's intentions and behaviour in terms of private information sharing [24,67,91], and provides a basis for future researchers to explore further the impact of gender on sustainable engagement with s-commerce, as well as other online activities where loss of online privacy represents a significant risk.

This study found, for example, that the impact of all our variables on intention and behaviour was higher in the case of females, but it does not provide detail on the reasons for that. The qualitative part of our investigation provides some insight into possible reasons

for the observations elsewhere in the literature (see Tifferet's review and meta-analysis [24]) that women have generally greater concern over privacy: we see female participants less likely to take the view that some risks in s-commerce are inevitable and to that extent are not worth worrying about. This observation also lends some support to Tifferet's [24] conclusion, after canvassing a range of possible explanations, that men's lower level of concern over privacy in social media generally is probably not explained by men having greater technical skill. Strikingly, however, if women's level of concern is higher, our results show that this is nonetheless more likely to combine with a higher intention to continue engagement. This may suggest that women will both be more demanding of platforms' addressing their privacy concerns and also be more optimistic that their demands will ultimately be met.

Perhaps unsurprisingly, the highest level of influence between factors in our model is between intention and behaviour. But the influence between these is also where we find the greatest gender difference (H8 in Table 8): women's expressed future intention to engage is much more likely to be consistent with their reported current engagement behaviour; men are more ambivalent about continuing their current practices in engaging with s-commerce. An explanation for this awaits further research, along with possible implications for a sensitivity to gender in approaches to sustainability of engagement with social commerce.

We are contributing to a more complete awareness of gender differences in the context of information sharing, which still needs further development. An improved understanding of these issues will have substantial practical implications. These will emerge especially in allowing social media and s-commerce platform designers to create privacy strategies and features that more effectively maximise adoption of, and sustainable engagement with, their services in the context, noted earlier, that the usage patterns (and markets) of many of these services are strongly differentiated by gender.

We noted above that s-commerce occurs within a social context that strongly conditions the risks and mitigations that are mediated by the technology. This context also strongly conditions users' perceptions, and it includes important aspects such as culture. We acknowledge that the present study, being carried out in Saudi Arabia, has a specific cultural setting which could influence the outcomes. Al-Omoush et al. [96] discuss extensively the impact of Arab culture on social commerce but have little to say directly about either gender or privacy. However, Zerbini et al. [13], based on a substantial review and meta-analysis, claim that "in individualistic and indulgent cultures, the effect of privacy concerns on intention diminishes": because Saudi Arabia is a relatively non-individualistic culture, this might suggest a more sustained concern with privacy risk. Moreover, the Saudi culture can give rise to relatively larger gender differences in various respects compared with some other cultures. This may include attitudes to privacy [38,97]. We note this, below, among the limitations of the study, but we note also that ultimately a broader picture across cultures will only emerge from comparing specific studies such as this one. A large cross-cultural study, even if it could be run, would be challenging to control any more effectively in terms of the complexity of the factors involved.

6.2. Managerial Implications

The findings of this study have several implications for social commerce managers. In the context of social commerce, perceived control of private information (PCPI) is a critical issue, especially for women. The literature establishes that women are more likely to be concerned about their privacy than men [24], and they are less likely to engage in social commerce if they do not feel confident that their private information will be protected. This is likely due to a number of factors; for example, women are more likely to be concerned about the potential for their personal information to be used for marketing purposes [98].

In addition to standard guidelines on transparency and the provision of privacy policies, we can make several recommendations:

1. Social commerce managers should focus on enhancing both Perceived Control of Private Information (PCPI) and the perceived benefits of social commerce in order to increase women's engagement. They should also consider the unique privacy concerns of women when designing their platforms and marketing campaigns.
2. Awareness and Acceptance of Privacy Policy (AAPP) is an important factor in user engagement, as users who are aware of and accept the privacy policy of a platform are more likely to engage with that platform. AAPP can be influenced by a number of factors, including the clarity of the privacy policy, the perceived trustworthiness of the platform and the user's own privacy concerns [5]. Gender is one of the factors that can influence AAPP, with women being more likely than men to be concerned about their privacy and less likely to accept privacy policies that they do not understand or trust [99,100]. Platforms should take gender into account when developing their privacy policies and marketing campaigns. They should make sure that their privacy policies are clear and concise, and that they address the specific privacy concerns of women. They should also build trust with women by being transparent about how their data are collected and used.
3. Managers should consider the target audience, the regulatory environment and the technological landscape when developing their privacy policies and marketing campaigns. The privacy concerns of different users may vary depending on their age, gender and location. Managers should tailor their privacy policies and marketing campaigns to the specific needs of their target audience.
4. Collection and Use of Personal Information (CUPI) is an important factor in user engagement, as users who are concerned about how their data will be used and shared are less likely to engage with a platform [8,24,38] unless they are effectively reassured that the platform protects their data. The effect of CUPI can be influenced by a number of factors, including the perceived trustworthiness of the platform, the user's own privacy concerns and the platform's privacy practices [101,102]. Platforms can address the appropriate scepticism inherent in CUPI by being transparent about how they collect and use data, by building trust with users and by taking steps to protect user privacy. Gender can play a role in CUPI, as different genders may have different privacy concerns. For example, a study by Mutambik et al. [38] found that women are more likely than men to be concerned about their personal information being used for marketing purposes. They are also more likely to be concerned about their personal information being used to track their online activity.

Managers can overall take a more general approach to addressing CUPI, recognising PCPI and justifying AAPP, by creating a culture of privacy within their organization. This includes educating employees about privacy issues and making sure that privacy is a top priority in all decision making. By taking these steps, managers can help to create a more trustworthy environment for users, which will work with privacy concerns and develop a strong and positive path towards more responsible and sustainable user engagement.

7. Conclusions and Limitations

Social commerce is a rapidly growing subsector of e-commerce, but it faces significant challenges, including issues of privacy, trust and ethics. This study set out to identify the key factors that have a significant impact on users' intention to share private information for the purpose of engaging in s-commerce. In particular, we sought to provide insights as to whether these factors vary with gender. In the study, we found three key aspects of privacy that influence ongoing user engagement with social commerce: Awareness and Acceptance of Privacy Policy (AAPP), Collection and Use of Personal Information (CUPI) and Perceived Control of Private Information (PCPI). Addressing our research questions (RQ1), we found that these three factors affect male and female participants to identifiably different extents (Table 8). Addressing RQ2, the study found a connection between these intentions and engagement behaviour, also reflecting the difference in strength by gender.

A theoretical question raised by this research is around the relative independence of CUIP and PCPI: one might speculate that concern about misuse of information would be tightly coupled to the perception of control over that information, yet these appear as independent constructs in our analysis (see Table 4). This warrants further investigation. The findings of this study have managerial and other implications for social media platforms and other social commerce providers, as noted in Section 6.2.

The findings of this study have also laid foundations for future research, as mentioned in Section 6.1, and pointed towards implications for other online contexts. The study could have benefitted from research into whether other (independent) control variables—e.g., ethnicity and cultural context—could impact sustainable consumer behaviour and could also have further explored other constructs, to confirm the full mediating impact of CUIP, PCPI and AAPP. Similarly, other variables such as whether the user normally uses a mobile device or a desktop could affect behaviour. However, at this stage, the focus adopted has allowed us to take a clear step forward. Other constructs could usefully be explored in future studies. Finally, it should be noted that the study uses a cross-sectional approach, which neglects the dynamic and evolving nature of attitudes to privacy, and that the research sample was focused on a single geographic region (Saudi Arabia). This could introduce a number of biases, such as sociocultural and economic biases. Further research in other cultural settings and perhaps with a larger, more contextually diverse, sample is therefore recommended.

Author Contributions: Conceptualization, I.M., J.L., A.A. (Abdullah Almuqrin), J.Z.Z. and M.B.; methodology, I.M., J.L., A.A. (Abdullah Almuqrin) and A.A. (Abdulrhman Alkhanifer); validation, A.A. (Abdulrhman Alkhanifer) and M.B.; formal analysis, A.A. (Abdullah Almuqrin); writing—original draft preparation, M.B.; writing—review and editing, I.M., J.L., A.A. (Abdulrhman Alkhanifer) and J.Z.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Researchers Supporting Project number (RSP2023R233), King Saud University, Riyadh, Saudi Arabia.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki and approved by the Institutional Review Board (Human and Social Researches) of King Saud University.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data are available on request due to restrictions of privacy.

Acknowledgments: This research was funded by the Researchers Supporting Project number (RSP2023R233), King Saud University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Statista. Value of Social Commerce Sales Worldwide from 2022 to 2026. Available online: <https://www.statista.com/statistics/1251145/social-commerce-sales-worldwide/> (accessed on 18 April 2021).
2. Statista. Leading Factors that Would Drive Online Shoppers Worldwide to Increase Their Use of Social Commerce in 2022. Available online: <https://www.statista.com/statistics/1275069/leading-drivers-social-commerce-use-increase/> (accessed on 18 April 2021).
3. Liang, T.-P.; Ho, Y.-T.; Li, Y.-W.; Turban, E. What Drives Social Commerce: The Role of Social Support and Relationship Quality. *Int. J. Electron. Commer.* **2011**, *16*, 69–90. [CrossRef]
4. Statista. Most Popular Social Commerce Platforms among Digital Buyers in the United States in 2022. Available online: <https://www.statista.com/statistics/250909/brand-engagement-of-us-online-shoppers-on-pinterest-and-facebook/> (accessed on 18 April 2021).
5. Mutambik, I.; Lee, J.; Almuqrin, A.; Zhang, J.Z.; Homadi, A. The Growth of Social Commerce: How It Is Affected by Users' Privacy Concerns. *J. Theor. Appl. Electron. Commer. Res.* **2023**, *18*, 725–743. [CrossRef]
6. Pan, B.; Guo, H.; You, X.; Xu, L. Privacy Rating of Mobile Applications Based on Crowdsourcing and Machine Learning. *J. Glob. Inf. Manag.* **2021**, *30*, 1–15. [CrossRef]
7. Florido-Benítez, L. International Mobile Marketing: A Satisfactory Concept for Companies and Users in Times of Pandemic. *Benchmarking Int. J.* **2022**, *29*, 1826–1856. [CrossRef]

8. Mutambik, I.; Almuqrin, A.; Liu, Y.; Alhossayin, M.; Quintash, F.H. Gender Differentials on Information Sharing and Privacy Concerns on Social Networking Sites: Perspectives From Users. *J. Glob. Inf. Manag.* **2021**, *29*, 236–255. [\[CrossRef\]](#)
9. Statista. Forecast Number of Mobile Devices Worldwide from 2020 to 2025. Available online: <https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/> (accessed on 18 April 2021).
10. Hajli, N.; Sims, J.; Zadeh, A.H.; Richard, M.-O. A Social Commerce Investigation of the Role of Trust in a Social Networking Site on Purchase Intentions. *J. Bus. Res.* **2017**, *71*, 133–141. [\[CrossRef\]](#)
11. Hajli, N. The Impact of Positive Valence and Negative Valence on Social Commerce Purchase Intention. *Inf. Technol. People* **2019**, *33*, 774–791. [\[CrossRef\]](#)
12. Chang, Y.; Wong, S.F.; Libaque-Saenz, C.F.; Lee, H. The Role of Privacy Policy on Consumers' Perceived Privacy. *Gov. Inf. Q.* **2018**, *35*, 445–459. [\[CrossRef\]](#)
13. Zerbini, C.; Bijmolt, T.H.A.; Maestripieri, S.; Luceri, B. Drivers of Consumer Adoption of E-Commerce: A Meta-Analysis. *Int. J. Res. Mark.* **2022**, *39*, 1186–1208. [\[CrossRef\]](#)
14. Alrawad, M.; Lutfi, A.; Alyatama, S.; Al Khattab, A.; Alsoboa, S.S.; Almaiah, M.A.; Ramadan, M.H.; Arafa, H.M.; Ahmed, N.A.; Alsyouf, A.; et al. Assessing Customers Perception of Online Shopping Risks: A Structural Equation Modeling-Based Multigroup Analysis. *J. Retail. Consum. Serv.* **2023**, *71*, 103188. [\[CrossRef\]](#)
15. Cao, J.; Everard, A. User Attitude Towards Instant Messaging: The Effect of Espoused National Cultural Values on Awareness and Privacy. *J. Glob. Inf. Technol. Manag.* **2008**, *11*, 30–57. [\[CrossRef\]](#)
16. Gorska, A.; Korzynski, P.; Mazurek, G.; Pucciarelli, F. The Role of Social Media in Scholarly Collaboration: An Enabler of International Research Team's Activation? *J. Glob. Inf. Technol. Manag.* **2020**, *23*, 273–291. [\[CrossRef\]](#)
17. Khandelwal, U.; Yadav, S.K.; Kumar, Y. Understanding Research Online Purchase Offline (ROPO) Behaviour of Indian Consumers. *Int. J. Online Mark.* **2020**, *10*, 1–14. [\[CrossRef\]](#)
18. Mutimukwe, C.; Kolkowska, E.; Grönlund, Å. Information Privacy in E-Service: Effect of Organizational Privacy Assurances on Individual Privacy Concerns, Perceptions, Trust and Self-Disclosure Behavior. *Gov. Inf. Q.* **2020**, *37*, 101413. [\[CrossRef\]](#)
19. Kizilcec, R.F.; Viberg, O.; Jivet, I.; Martinez Mones, A.; Oh, A.; Hrastinski, S.; Mutimukwe, C.; Scheffel, M. The Role of Gender in Students' Privacy Concerns about Learning Analytics. In Proceedings of the LAK23: 13th International Learning Analytics and Knowledge Conference, Arlington, TX, USA, 13–17 March 2023; ACM: New York, NY, USA, 2023; pp. 545–551. [\[CrossRef\]](#)
20. Wang, Y.; Herrando, C. Does Privacy Assurance on Social Commerce Sites Matter to Millennials? *Int. J. Inf. Manag.* **2019**, *44*, 164–177. [\[CrossRef\]](#)
21. Mitchell, D.; El-Gayar, O. The Effect of Privacy Policies on Information Sharing Behavior on Social Networks: A Systematic Literature Review. In Proceedings of the 53rd Hawaii International Conference on System Sciences, Maui, HI, USA, 7–10 January 2020. [\[CrossRef\]](#)
22. Maor, W.; Maayan, Z.G.; Dan, B. Sex Differences in Attitudes towards Online Privacy and Anonymity among Israeli Students with Different Technical Backgrounds. *arXiv* **2017**, arXiv:2308.03814. [\[CrossRef\]](#)
23. Hoy, M.G.; Milne, G. Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *J. Interact. Advert.* **2010**, *10*, 28–45. [\[CrossRef\]](#)
24. Tifferet, S. Gender Differences in Privacy Tendencies on Social Network Sites: A Meta-Analysis. *Comput. Hum. Behav.* **2019**, *93*, 1–12. [\[CrossRef\]](#)
25. Rowan, M.; Dehlinger, J. Observed Gender Differences in Privacy Concerns and Behaviors of Mobile Device End Users. *Procedia Comput. Sci.* **2014**, *37*, 340–347. [\[CrossRef\]](#)
26. Sørum, H.; Eg, R.; Presthus, W. A Gender Perspective on GDPR and Information Privacy. *Procedia Comput. Sci.* **2022**, *196*, 175–182. [\[CrossRef\]](#)
27. Salvatori, L.; Marcantoni, F. Social Commerce: A Literature Review. In Proceedings of the 2015 Science and Information Conference (SAI), London, UK, 28–30 July 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 257–262. [\[CrossRef\]](#)
28. McKinsey. Browsing and Shopping Directly on Social Media Platforms Is a Core Feature of E-Commerce in China. Now, This Dynamic New Way of Buying Is Poised for Rapid Growth in the United States. Available online: <https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/social-commerce-the-future-of-how-consumers-interact-with-brands> (accessed on 18 April 2021).
29. Ziyadin, S.; Doszhan, R.; Borodin, A.; Omarova, A.; Ilyas, A. The Role of Social Media Marketing in Consumer Behaviour. *E3S Web Conf.* **2019**, *135*, 04022. [\[CrossRef\]](#)
30. Yan, J.; Zhang, S.; Zhang, S. Emotional Attachment in Social E-Commerce: The Role of Social Capital and Peer Influence. *Sustainability* **2023**, *15*, 4792. [\[CrossRef\]](#)
31. Quan-Haase, A.; Ho, D. Online Privacy Concerns and Privacy Protection Strategies among Older Adults in East York, Canada. *J. Assoc. Inf. Sci. Technol.* **2020**, *71*, 1089–1102. [\[CrossRef\]](#)
32. Kruikemeier, S.; Boerman, S.C.; Bol, N. Breaching the Contract? Using Social Contract Theory to Explain Individuals' Online Behavior to Safeguard Privacy. *Media Psychol.* **2020**, *23*, 269–292. [\[CrossRef\]](#)
33. Barth, S.; Ionita, D.; Hartel, P. Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines. *ACM Comput. Surv.* **2023**, *55*, 1–37. [\[CrossRef\]](#)
34. Xu, Z.; Xiang, D.; He, J. Data Privacy Protection in News Crowdfunding in the Era of Artificial Intelligence. *J. Glob. Inf. Manag.* **2022**, *30*, 1–17. [\[CrossRef\]](#)

35. Al-Qirim, N.; Rouibah, K.; Abbas, H.; Hwang, Y. Factors Affecting the Success of Social Commerce in Kuwaiti Microbusinesses: A Qualitative Study. *J. Glob. Inf. Manag.* **2022**, *30*, 1–31. [\[CrossRef\]](#)
36. Gerber, N.; Gerber, P.; Volkamer, M. Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. *Comput. Secur.* **2018**, *77*, 226–261. [\[CrossRef\]](#)
37. Li, C.; Chu, J.; Zheng, L.J. Better Not Let Me Know: Consumer Response to Reported Misuse of Personal Data in Privacy Regulation. *J. Glob. Inf. Manag.* **2022**, *30*, 1–22. [\[CrossRef\]](#)
38. Mutambik, I.; Lee, J.; Almuqrin, A.; Halboob, W.; Omar, T.; Floos, A. User Concerns Regarding Information Sharing on Social Networking Sites: The User's Perspective in the Context of National Culture. *PLoS ONE* **2022**, *17*, e0263157. [\[CrossRef\]](#)
39. Venkatesh, V.; Speier, C.; Morris, M.G. User Acceptance Enablers in Individual Decision Making About Technology: Toward an Integrated Model. *Decis. Sci.* **2002**, *33*, 297–316. [\[CrossRef\]](#)
40. Fortes, N.; Rita, P. Privacy Concerns and Online Purchasing Behaviour: Towards an Integrated Model. *Eur. Res. Manag. Bus. Econ.* **2016**, *22*, 167–176. [\[CrossRef\]](#)
41. Wang, L.-Y.; Hu, H.-H.; Wang, L.; Qin, J.-Q. Privacy Assurances and Social Sharing in Social Commerce: The Mediating Role of Threat-Coping Appraisals. *J. Retail. Consum. Serv.* **2022**, *67*, 103028. [\[CrossRef\]](#)
42. Zhou, T. The Effect of Information Privacy Concern on Users' Social Shopping Intention. *Online Inf. Rev.* **2020**, *44*, 1119–1133. [\[CrossRef\]](#)
43. Culnan, M.J.; Bies, R.J. Consumer Privacy: Balancing Economic and Justice Considerations. *J. Soc. Issues* **2003**, *59*, 323–342. [\[CrossRef\]](#)
44. Meso, P.; Negash, S.; Musa, P.F. Interactions Between Culture, Regulatory Structure, and Information Privacy Across Countries. *J. Glob. Inf. Manag.* **2021**, *29*, 1–14. [\[CrossRef\]](#)
45. Libaque-Sáenz, C.F.; Wong, S.F.; Chang, Y.; Bravo, E.R. The Effect of Fair Information Practices and Data Collection Methods on Privacy-Related Behaviors: A Study of Mobile Apps. *Inf. Manag.* **2020**, *58*, 103284. [\[CrossRef\]](#)
46. Jacobson, J.; Gruz, A.; Hernández-García, Á. Social Media Marketing: Who Is Watching the Watchers? *J. Retail. Consum. Serv.* **2020**, *53*, 101774. [\[CrossRef\]](#)
47. Jozani, M.; Ayaburi, E.; Ko, M.; Choo, K.-K.R. Privacy Concerns and Benefits of Engagement with Social Media-Enabled Apps: A Privacy Calculus Perspective. *Comput. Hum. Behav.* **2020**, *107*, 106260. [\[CrossRef\]](#)
48. Smith, H.J.; Milberg, S.J.; Burke, S.J. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Q.* **1996**, *20*, 167–196. [\[CrossRef\]](#)
49. Malhotra, N.K.; Kim, S.S.; Agarwal, J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Inf. Syst. Res.* **2004**, *15*, 336–355. [\[CrossRef\]](#)
50. Fogel, J.; Nehmad, E. Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns. *Comput. Hum. Behav.* **2009**, *25*, 153–160. [\[CrossRef\]](#)
51. Feng, Y.; Xie, W. Teens' Concern for Privacy When Using Social Networking Sites: An Analysis of Socialization Agents and Relationships with Privacy-Protecting Behaviors. *Comput. Hum. Behav.* **2014**, *33*, 153–162. [\[CrossRef\]](#)
52. Almuqrin, A.; Mutambik, I. The Explanatory Power of Social Cognitive Theory in Determining Knowledge Sharing among Saudi Faculty. *PLoS ONE* **2021**, *16*, e0248275. [\[CrossRef\]](#) [\[PubMed\]](#)
53. Biselli, T.; Steinbrink, E.; Herbert, F.; Schmidbauer-Wolf, G.M.; Reuter, C. On the Challenges of Developing a Concise Questionnaire to Identify Privacy Personas. *Proc. Priv. Enhancing Technol.* **2022**, *2022*, 645–669. [\[CrossRef\]](#)
54. Johnson, R.B.; Onwuegbuzie, A.J. Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educ. Res.* **2004**, *33*, 14–26. [\[CrossRef\]](#)
55. Braun, V.; Clarke, V. Using Thematic Analysis in Psychology. *Qual. Res. Psychol.* **2006**, *3*, 77–101. [\[CrossRef\]](#)
56. Saunders, B.; Sim, J.; Kingstone, T.; Baker, S.; Waterfield, J.; Bartlam, B.; Burroughs, H.; Jinks, C. Saturation in Qualitative Research: Exploring Its Conceptualization and Operationalization. *Qual. Quant.* **2018**, *52*, 1893–1907. [\[CrossRef\]](#)
57. Fishbein, M.; Ajzen, I. *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research*; Addison-Wesley: Reading, MA, USA, 1975.
58. Chen, Y.; Zahedi, F.M. Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Q.* **2016**, *40*, 205–222. [\[CrossRef\]](#)
59. Yu, L.; Li, H.; He, W.; Wang, F.-K.; Jiao, S. A Meta-Analysis to Explore Privacy Cognition and Information Disclosure of Internet Users. *Int. J. Inf. Manag.* **2020**, *51*, 102015. [\[CrossRef\]](#)
60. Smith, H.J.; Dinev, T.; Xu, H. Information Privacy Research: An Interdisciplinary Review. *MIS Q.* **2011**, *35*, 989–1015. [\[CrossRef\]](#)
61. Gillespie, N.; Dietz, G. Trust Repair After An Organization-Level Failure. *Acad. Manag. Rev.* **2009**, *34*, 127–145. [\[CrossRef\]](#)
62. Ayaburi, E.W.; Treku, D.N. Effect of Penitence on Social Media Trust and Privacy Concerns: The Case of Facebook. *Int. J. Inf. Manag.* **2020**, *50*, 171–181. [\[CrossRef\]](#)
63. Youn, S. Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *J. Consum. Aff.* **2009**, *43*, 389–418. [\[CrossRef\]](#)
64. Huang, J.; Kumar, S.; Hu, C. Gender Differences in Motivations for Identity Reconstruction on Social Network Sites. *Int. J. Hum. Comput. Interact.* **2018**, *34*, 591–602. [\[CrossRef\]](#)
65. Kisilevich, S.; Ang, C.S.; Last, M. Large-Scale Analysis of Self-Disclosure Patterns among Online Social Networks Users: A Russian Context. *Knowl. Inf. Syst.* **2012**, *32*, 609–628. [\[CrossRef\]](#)

66. Benamati, J.H.; Ozdemir, Z.D.; Smith, H.J. Information Privacy, Cultural Values, and Regulatory Preferences. *J. Glob. Inf. Manag.* **2021**, *29*, 131–164. [\[CrossRef\]](#)
67. Kwahk, K.-Y.; Park, D.-H. The Effects of Network Sharing on Knowledge-Sharing Activities and Job Performance in Enterprise Social Media Environments. *Comput. Hum. Behav.* **2016**, *55*, 826–839. [\[CrossRef\]](#)
68. Tufekci, Z. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bull. Sci. Technol. Soc.* **2008**, *28*, 20–36. [\[CrossRef\]](#)
69. Krasnova, H.; Spiekermann, S.; Koroleva, K.; Hildebrand, T. Online Social Networks: Why We Disclose. *J. Inf. Technol.* **2010**, *25*, 109–125. [\[CrossRef\]](#)
70. Lin, X.; Brooks, S. Factors Affecting Online Consumer's Behavior: An Investigation Across Gender. In Proceedings of the 19th Americas Conference on Information Systems, Chicago, IL, USA, 15–17 August 2013.
71. Almuqrin, A.; Zhang, Z.; Alzamil, A.; Mutambik, I.; Alhabeeb, A. The Explanatory Power of Social Capital in Determining Knowledge Sharing in Higher Education: A Case from Saudi Arabia. *Malays. J. Libr. Inf. Sci.* **2020**, *25*, 71–90. [\[CrossRef\]](#)
72. Lin, X.; Li, Y.; Califf, C.B.; Featherman, M. Can Social Role Theory Explain Gender Differences in Facebook Usage? In Proceedings of the 2013 46th Hawaii International Conference on System Sciences, Wailea, HI, USA, 7–10 January 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 690–699. [\[CrossRef\]](#)
73. Sun, S.; Drake, J.R.; Hall, D. When Job Candidates Experience Social Media Privacy Violations. *J. Glob. Inf. Manag.* **2022**, *30*, 1–25. [\[CrossRef\]](#)
74. Rigdon, E.E.; Sarstedt, M.; Ringle, C.M. On Comparing Results from CB-SEM and PLS-SEM: Five Perspectives and Five Recommendations. *Mark. ZFP* **2017**, *39*, 4–16. [\[CrossRef\]](#)
75. Afthanorhan, A.; Awang, Z.; Aimran, N. An Extensive Comparison of CB-SEM and PLS-SEM for Reliability and Validity. *Int. J. Data Netw. Sci.* **2020**, 357–364. [\[CrossRef\]](#)
76. MacKenzie, S.B.; Podsakoff, P.M.; Podsakoff, N.P. Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques. *MIS Q.* **2011**, *35*, 293–334. [\[CrossRef\]](#)
77. Straub, D.; Gefen, D. Validation Guidelines for IS Positivist Research. *Commun. Assoc. Inf. Syst.* **2004**, *13*, 24. [\[CrossRef\]](#)
78. Purwanto, A.; Asbari, M.; Santoso, T.I.; Sunarsi, D.; Ilham, D. Education Research Quantitative Analysis for Little Respondents. *J. Studi Guru Dan Pembelajaran* **2021**, *4*, 335–350. [\[CrossRef\]](#)
79. Donmez-Turan, A. Does Unified Theory of Acceptance and Use of Technology (UTAUT) Reduce Resistance and Anxiety of Individuals towards a New System? *Kybernetes* **2019**, *49*, 1381–1405. [\[CrossRef\]](#)
80. Creswell, J.W.; Clark, V.L.P. *Designing and Conducting Mixed Methods Research*; SAGE: London, UK, 2011.
81. Hair, J.F.; Ringle, C.M.; Sarstedt, M. PLS-SEM: Indeed a Silver Bullet. *J. Mark. Theory Pract.* **2011**, *19*, 139–152. [\[CrossRef\]](#)
82. Hair, J.F., Jr.; Matthews, L.M.; Matthews, R.L.; Sarstedt, M. PLS-SEM or CB-SEM: Updated Guidelines on Which Method to Use. *Int. J. Multivar. Data Anal.* **2017**, *1*, 107–123. [\[CrossRef\]](#)
83. Fornell, C.; Larcker, D.F. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *J. Mark. Res.* **1981**, *18*, 39–50. [\[CrossRef\]](#)
84. Chin, W.W. The Partial Least Squares Approach to Structural Equation Modeling. *Mod. Methods Bus. Res.* **1998**, *295*, 295–336.
85. Gefen, D.; Straub, D. The Relative Importance of Perceived Ease of Use in IS Adoption: A Study of E-Commerce Adoption. *J. Assoc. Inf. Syst.* **2000**, *1*, 8. [\[CrossRef\]](#)
86. Schumacker, R.E.; Lomax, R.G. *A Beginner's Guide to Structural Equation Modeling*, 3rd ed.; Routledge/Taylor & Francis Group: Oxford, UK, 2010.
87. Keil, M.; Tan, B.C.Y.; Wei, K.-K.; Saarinen, T.; Tuunainen, V.; Wassenaar, A. A Cross-Cultural Study on Escalation of Commitment Behavior in Software Projects. *MIS Q.* **2000**, *24*, 299–325. [\[CrossRef\]](#)
88. Ahuja, M.K.; Thatcher, J.B. Moving beyond Intentions and toward the Theory of Trying: Effects of Work Environment and Gender on Post-Adoption Information Technology Use. *MIS Q.* **2005**, *29*, 427–459. [\[CrossRef\]](#)
89. Michaelidou, N.; Micevski, M.; Cadogan, J.W. Users' Ethical Perceptions of Social Media Research: Conceptualisation and Measurement. *J. Bus. Res.* **2020**, *124*, 684–694. [\[CrossRef\]](#)
90. Mousavi, R.; Chen, R.; Kim, D.J.; Chen, K. Effectiveness of Privacy Assurance Mechanisms in Users' Privacy Protection on Social Networking Sites from the Perspective of Protection Motivation Theory. *Decis. Support Syst.* **2020**, *135*, 113323. [\[CrossRef\]](#)
91. Berings, D.; Adriaenssens, S. The Role of Business Ethics, Personality, Work Values and Gender in Vocational Interests from Adolescents. *J. Bus. Ethics* **2012**, *106*, 325–335. [\[CrossRef\]](#)
92. Pandey, J.; Hassan, Y. Batting Outside the Field: Examining E-Engagement Behaviors of IPL Fans. *J. Glob. Inf. Manag.* **2021**, *30*, 1–17. [\[CrossRef\]](#)
93. Chang, S.E.; Liu, A.Y.; Shen, W.C. User Trust in Social Networking Services: A Comparison of Facebook and LinkedIn. *Comput. Hum. Behav.* **2017**, *69*, 207–217. [\[CrossRef\]](#)
94. Wu, K.-W.; Huang, S.Y.; Yen, D.C.; Popova, I. The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust. *Comput. Hum. Behav.* **2012**, *28*, 889–897. [\[CrossRef\]](#)
95. Oliveira, T.; Araujo, B.; Tam, C. Why Do People Share Their Travel Experiences on Social Media? *Tour. Manag.* **2020**, *78*, 104041. [\[CrossRef\]](#)
96. Al-Omoush, K.S.; Ancillo, A.d.L.; Gavrila, S.G. The Role of Cultural Values in Social Commerce Adoption in the Arab World: An Empirical Study. *Technol. Forecast. Soc. Change* **2022**, *176*, 121440. [\[CrossRef\]](#)

97. Wang, X.W.; Riaz, M.; Haider, S.; Alam, K.M.; Sherani, Yang, M. Information Sharing on Social Media by Multicultural Individuals. *J. Glob. Inf. Manag.* **2021**, *29*, 1–25. [[CrossRef](#)]
98. Goyal, S.; Hu, C.; Chauhan, S.; Gupta, P.; Bhardwaj, A.K.; Mahindroo, A. Social Commerce: A Bibliometric Analysis and Future Research Directions. *J. Glob. Inf. Manag.* **2022**, *29*, 1–33. [[CrossRef](#)]
99. Rouibah, K.; Al-Qirim, N.; Hwang, Y.; Pouri, S.G. The Determinants of EWOM in Social Commerce: The Role of Perceived Value, Perceived Enjoyment, Trust, Risks, and Satisfaction. *J. Glob. Inf. Manag.* **2021**, *29*, 75–102. [[CrossRef](#)]
100. Sohaib, O. Social Networking Services and Social Trust in Social Commerce: A PLS-SEM Approach. *J. Glob. Inf. Manag.* **2021**, *29*, 23–44. [[CrossRef](#)]
101. Malhan, M.; Dewani, P.P.; Nigam, A.; Vaz, D.; Ogbeibu, E.A.A. Exploring Customer Engagement on Social Networking Sites. *J. Glob. Inf. Manag.* **2022**, *30*, 1–28. [[CrossRef](#)]
102. Almuqrin, A.; Mutambik, I.; Alomran, A.; Gauthier, J.; Abusharhah, M. Factors Influencing Public Trust in Open Government Data. *Sustainability* **2022**, *14*, 9765. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.