digital

MDPI

Article

Re-Evaluating Trust and Privacy Concerns When Purchasing a Mobile App: Re-Calibrating for the Increasing Role of Artificial Intelligence

Alex Zarifis [1,*] and Shixuan Fu [2]

[1] Department of Management and Information Systems, PSL Research University, 75006 Paris, France
[2] School of Economics & Management, University of Science and Technology Beijing, Beijing 100083, China
* Correspondence: alex.zarifis@dauphine.psl.eu

Abstract: Mobile apps utilize the features of a mobile device to offer an ever-growing range of functionalities. This vast choice of functionalities is usually available for a small fee or for free. These apps access the user's personal data, utilizing both the sensors on the device and big data from several sources. Nowadays, Artificial Intelligence (AI) is enhancing the ability to utilize more data and gain deeper insight. This increase in the access and utilization of personal information offers benefits but also challenges to trust. Using questionnaire data from Germany, this research explores the role of trust from the consumer's perspective when purchasing mobile apps with enhanced AI. Models of trust from e-commerce are adapted to this specific context. A model is proposed and explored with quantitative methods. Structural Equation Modeling enables the relatively complex model to be tested and supported. Propensity to trust, institution-based trust, perceived sensitivity of personal information, and trust in the mobile app are found to impact the intention to use the mobile app with enhanced AI.

Keywords: trust; information privacy; artificial intelligence; mobile commerce; mobile apps; big data

check for updates

Citation: Zarifis, A.; Fu, S. Re-Evaluating Trust and Privacy Concerns When Purchasing a Mobile App: Re-Calibrating for the Increasing Role of Artificial Intelligence. *Digital* **2023**, *3*, 286–299. https://doi.org/10.3390/digital3040018

Academic Editor: Emiliano Tramontana

Received: 15 August 2023
Revised: 13 September 2023
Accepted: 6 October 2023
Published: 13 October 2023

1. Introduction

Mobile e-commerce is widely adopted, and it is constantly evolving following developments in technology, society and the business models implemented online. Mobile commerce is increasingly popular either as a single platform or as part of a multichannel interaction. As a multichannel interaction, it can combine traditional physical stores, online websites with two-dimensional navigation, online websites with three-dimensional navigation and applications specialized for mobile devices. The increasing development of Artificial Intelligence (AI) and big data techniques also bring new opportunities to mobile e-commerce. For example, AI tools can create elaborate recommendations combining several products and services and communicate this in human-like speech. However, mobile devices have relative weaknesses such as smaller screens and relative advantages such as access to the user's personal information, including their location. The consumer, who is also a user of technology, has a similar but distinct experience on these different channels [1]. The factors influencing whether the consumer will trust the vendor sufficiently to make a purchase are also similar but distinct. With the far-reaching changes to the technology the consumer engages with when purchasing a mobile app, the existing models of trust may be outdated and not entirely accurate. Therefore, this research re-evaluates trust and privacy concerns when purchasing a mobile app to take into account the current environment that uses AI extensively.

E-commerce increases the speed of the transaction and decreases the costs, reshaping the purchasing behavior of the consumer. The consumer is presented with many choices before making a final purchasing decision. Product quality and competitive pricing might have been dominant factors to drive a purchasing decision in the past, but as the consumer becomes more demanding online, other factors such as online reviews, product rating, website reputation, secure payment process, secure handling of personal information, natural language processing and website design also influence the buying decision online [2,3].

Due to the nature of e-commerce in which the seller and buyer are physically separate and lack the visual cues, trust is recognized as a critical factor to foster the relationship between vendors and customers [4]. In e-commerce, the consumer is faced with several technologies and organizations from the time they start inquiring about a mobile app to the time they purchase it. These layers of technologies and business models each have their own risks and require trust from the consumer. A simple example is that a consumer may trust the developer of the app, but not the platform offering it, and may therefore try to find the app elsewhere to purchase it. Therefore, while some research approaches trust by trying to capture it in the simplest way possible by grouping the issues influencing trust into a small number of factors, it is necessary to incorporate the related trust issues of all the layers to comprehensively model it. This is analogous to the evolution from TAM to the more comprehensive UTAUT2 [5]. Consequently, this research explores the consumer's trust and privacy concern when using a mobile device to purchase a mobile app. This context combines elements of e-commerce, as this is an online purchase, and technology adoption, as what is being considered for purchase is a mobile app.

Many retailers offer mobile apps that combine several functions including offering points that can be used to purchase products and are therefore a form of payment. They also collect what we are consuming, which is an indication of our health. Therefore, the lines between payment methods, entertainment applications and membership applications are no longer clear.

Gaining and maintaining trust can be a challenging task for many organizations in this virtual market. There are different types of trust such as trust in AI [6], trust in virtual collaboration [7] and trust in a payment method [8]. These different applications of trust share common characteristics but also have some differences that are caused by their context. Trust in e-commerce has been researched extensively and can be considered mature. However, the network of technologies available to consumers is evolving. This causes consumers' relationship with these networks of technology to evolve, which leads to changes in the nature of trust in e-commerce. The criteria for trust is shifting from trust in the vendor and the quality of the product or service to how the personal information such as browsing history, banking details, purchase history and GPS history is being used by AI and big data. Personal information privacy concern is not something new, but the increased pervasiveness of the technologies collecting information and the capability of AI to harness this information have made this issue more prominent [9,10]. Purchasing an app on a mobile phone brings together a specific combination of characteristics and thus a different form of trust. McKnight [11] proposed a model specifically for trust in technology as opposed to between people or organizations such as the consumer and the vendor. The model proposed by McKnight [11] is more focused and more suitable, but it still needs to be adapted further and extended to capture trust, in this context, as comprehensively and accurately as possible. This model was created and proposed as a basic model of trust in technology that would then need to be adapted to different types of technologies. In the specific context explored here, the technology can be considered central, but there are, nevertheless, still relationships among people such as the vendor and the consumer that need to be covered. Therefore, the research question is:

What are the factors affecting a consumer's trust when making a purchase of a mobile app online?

The focus is on both the technical and social aspects that influence trust and privacy concern when a consumer purchases a mobile app. Consumers who have experience in purchasing mobile apps were recruited as participants. A better understanding of the decision-making behavior significantly enhances e-commerce as well as mobile commerce by improving the online platforms and information systems that enable this process.

The findings identify propensity to trust, institutional trust, perceived sensitivity of the personal information and the trusting beliefs in the mobile app as factors influencing the intention to use. The next section covers the theoretical foundation and how the hypotheses were developed. The methodology section follows, explaining the quantitative methods of data collection and analysis that were implemented. This is followed by the analysis of the data and the discussion of the results. Lastly, the conclusion summarizes the insight gained in this research.

2. Theoretical Foundation

The behavior of consumers in mobile commerce is influenced by several areas that can be best summarized by reviewing the general e-commerce landscape, the specific characteristics of purchasing online, mobile commerce and, lastly, the role of trust in terms of e-commerce, mobile commerce and technology adoption.

In some scenarios, the increasing role of AI may be obvious, such as when a consumer is interacting with an AI chat-bot. In other scenarios, the consumer does not interact directly with the AI and just completes some online forms. Despite not interacting with the AI directly, it is still used to deliver the service. Therefore, alongside the studies that measure direct interaction with AI, other scenarios, such as purchasing mobile apps, where AI is influential despite not being the main issue, must also be re-evaluated.

The consumer's trust in mobile apps is tested by malware and other cybersecurity threats [12,13]. An additional challenge to trust is fraud, where the purpose is typically to steal money or the consumer's personal information [14].

Consumer trust is dependent on three parameters: (a) a specific person's psychology [11,15,16], (b) the institutions that have a role in ensuring that the risks involved in using a technology are reduced [17,18], and (c) the technology they are interacting with [11,19]. A fourth issue that plays a role is (d) the consumer's concern about the personal information being shared [20,21]. Some of the literature supporting the three dimensions of trust and privacy concerns is presented in Table 1. All four of these parameters are influenced in some way by the extremely disruptive digital transformation being driven by AI.

Table 1. Literature on dimensions of trust.

Dimensions of Trust	Related Literature
Each person's psychology	McKnight et al. 2011 [11], Kim & Prabhakar, 2004 [15], Bansal et al. 2010 [16]
Institutions that reduce the risks in using a technology	Vance et al. 2008 [17], Zhang et al. 2015 [18]
The dimensions of the technology that influence trust	Lankton et al. 2015 [19], McKnight et al. 2011 [11]
Personal information privacy concern when using a specific technology	Degutis et al. 2023 [20]; Pang & Ruan, 2023 [21]

Hypotheses Development

Based on the literature, some factors are considered to influence trust and the intention to use. The intention to use affects the buying decision. These factors and effects are captured in thirteen hypotheses. This large number of hypotheses is necessary to cover the user's perspective comprehensively. The factors outlined below include the individual's trusting stance, textual presentation of the app, video presentation of the app, the product reviews of the app, the average rating of the app, transparent information on an existing vendor, a free-trial version, the app being promoted by a platform in an app market such as for example Samsung Galaxy Store, institutional trust in the web, humanness of the technology and personal information sensitivity.

Propensity to trust: It has been validated extensively that propensity to trust [15] and similar concepts such as trusting stance [11] and disposition to trust [16] influence other factors that play a role in building personal trust. Trusting stance means the consumer believes that if they show trust, there will be a positive outcome regardless of how trustworthy the technology is. Faith in general technology means the consumer believes that, in general, technology is reliable and will perform as expected. People have different personalities and experiences that shape their predisposition toward trusting. It is therefore a valid starting point when modeling trust in a specific context. Propensity to trust is formed by the user's personal trusting stance and their general faith in technology. Therefore, the first three hypotheses follow:

H1. *Trusting stance positively affects propensity to trust.*

H2. *Faith in general technology positively affects propensity to trust.*

H3. *Propensity to trust positively affects institution-based trust.*

Structural Assurance: This includes guarantees, regulation, promises and related laws which are in place to protect the consumer in an e-commerce context [17,18]. These safeguards encourage the consumer to believe the vendor's website is secure and safe to make a transaction. The more indications of structural assurance the consumer is exposed to, the stronger the trust. This form of trust can be supported with technology infrastructure such as encryption or secure socket layer (SSL) to protect from a harmful online attack [22]. Embedding accredited seals of approval such as Norton Secured and McAfee Secure [23] further supports trust.

H4. *Structural assurance in the internet positively affects institution-based trust.*

Situational normality: In order to learn about the performance of a product and reduce the risk, the consumer is relying more on reviews of products written by other consumers [24]. A product review is usually a qualitative assessment in which a consumer expresses their opinion of a product [25]. A balanced review indicates that the consumer is not biased in their opinion and is being honest in their feedback. Similar to the product review, a rating review is a quantitative evaluation in which the consumer rates the performance of a product, which is often based on a numeric scale starting from 1 (worst) to 5 (best) [25]. As a consumer is often overwhelmed and bombarded by a huge amount of product variation, a rating scheme can help them to reduce the set of products to consider [26]. Reviews and ratings develop the consumer's belief in situational normality.

H5. *Situational normality positively affects trusting beliefs on institution-based trust.*

H6. *Institution-based trust positively affects trusting beliefs in a mobile app.*

Trust in vendor: In mobile commerce, the consumer faces several risks. For example, even downloading the app may have problems due to the internet connection. In addition, by its nature, the mobile app itself is very different from a tangible product. After buying the app, the consumer does not have the privilege of returning the app as they do when buying other products such as books or clothes. As a result, the consumer needs to have transparent information about their vendor which makes them trust and believe that they are doing business with a legitimate business entity rather than an unknown one [27]. Most of the mobile app vendors have the information about their company displayed on platforms like Google Play. The information might include the website and address of the vendor. Furthermore, it is important for the reputation of an online vendor to have a long record of fulfilling what they have claimed online [28]. The reputation plays an essential role in retaining the consumer, reducing information asymmetry and increasing their acceptance of e-commerce:

H7. *Trust in the vendor positively affects trusting belief in a mobile app.*

Trust in app functionality: The consumer being educated about the functionality though a video and experiencing the functionality through a free version can help build trust. A video presentation sharing information on the app could help the consumer visualize how it might perform and offer a sensory product experience [29]. A visual online product presentation can help the consumer effectively recall the product attributes and positively affect their confidence [30]. The visual online product presentation contains pictorial and graphical information, which enables a sensory encoding process to facilitate the retrieval of information from the working memory of a consumer and then influence their recall and recognition. Since the products cannot be felt or touched in a virtual environment, a video supports the evaluation of a product [29].

A free trial version refers to an app which is provided free of charge but with limited functionalities or with full function for a limited time [31]. The purpose of the free trial is to attract the consumer and allow them to gain some initial experience, so they form a positive opinion and pay the fee to continue to use the app [31,32]. The free trial version could form the initial trust, since a software app is an intangible product which the consumer cannot touch or feel, but the consumer needs to have an experience of it in order to assess the quality [31,33]. In addition, the free trial not only makes the consumer quickly adopt the app, but it also speeds up the process of them becoming familiar with the app [31,34]. After experiencing the app, the consumer can become more confident in their decision based on the merit of the app instead of trying to base their decision on advertising [31,34].

H8. *Trust in the reliability of the mobile app functionality positively affects trusting belief in a mobile app.*

Trust in the genuineness of the app: In mobile commerce, where customers do not have an opportunity to physically experience or touch the product, the textual presentation of an item has an important role in conveying a message to the consumer which enhances their understanding of it [30]. Therefore, a concise and accurate description reduces the uncertainty about what the app is and increases trust. Mobile apps developed by individuals, or organizations, are usually purchased through distribution platforms such as Google Play. These reputable distribution platforms carefully review and test apps before they offer them. According to statistics from BitDefender, in 2022, only 35 out of over 3.5 million apps on Google Play were harmful and caused security risks to the user's data [35]. Distribution platforms try to keep the consumer's device away from harmful apps so that people feel safe when purchasing an app from their platform. The textual representation and distribution platform shape the perception of the genuineness of the app.

H9. *Trust in the genuineness of the app positively affects the trusting belief in a mobile app.*

Technology humanness: Research on trust in information systems has primarily focused on how the user perceives the technical characteristics of the system, following the literature on technology adoption. As technology is increasingly being used as a platform for social interaction, the humanness or human-like nature of the technology influences trust in parallel with the characteristics that are more closely related to the technical attributes that describe a technology as a tool [19]. It has been posited that in technologies with strong humanness, trust is influenced primarily from the humanness with the more technology attribute-related trust having a secondary role [19]. As some mobile apps combine many functionalities, the context where humanness is the primary or secondary form of trust could both occur within one app. Therefore, for a model of trust to be comprehensive, the primary characteristics of the human-focused trust should be included along with the more technology attribute-oriented ones. Integrity, competence and benevolence are posited to influence the human-focused trust [19].

H10. *A technology that is perceived to have a higher humanness positively affects the trusting belief in a mobile app.*

Trust in personal data use: Personal information can be considered as the fuel of the modern economy and the primary currency of the time we are living in. While the importance and value of data cannot be disputed, the consumer providing their information may have reservations about how these data are used and whether their privacy is compromised [36]. Some information is more sensitive such as information directly, or indirectly, related to finance or health [16,37]. As a person brings their disposition to trust to each different situation requiring trust, a person also brings with them a perception of how sensitive their personal information is.

H11. *A high perceived sensitivity of personal information negatively affects trust in personal data use.*

Apps for mobile devices collect information from the device's software and sensors such as location, browsing history [38] and purchasing history both online and in physical stores, for example using Samsung Pay [3]. This leads to them collecting information that is sensitive for the consumer both in isolation and when combined with other information through big data analysis. There is an increasing number of sensors on mobile devices and in our environment, collecting information. Additionally, AI is becoming more effective in bringing personal data together from several sources, analyzing it, and applying the decision in a fully automated way. These personal data can also be legitimately passed onto third parties or leaked to them due to negligence. What is collected may also be inaccurate [39]. Therefore, while trust in the responsible use of data was always important, its importance is increasing as the volume of personal data shared grows and the capabilities to utilize personal data also increase.

H12: *Trust in the responsible use of personal data positively affects the trusting belief in a mobile app.*

Intention to use mobile app: According to the theory of reasoned action, human behavior could be predicted by the intentions which are influenced by attitude toward the behavior and the subjective norm [40]. In other words, intention is a powerful indicator to predict an individual's behavior [41]. Intention is the willingness of an individual to conduct a certain action [41]. Therefore, the trusting beliefs of the consumer in the mobile app should positively influence their intention to use.

H13:*A trusting belief in a mobile app positively affects intention to use a mobile app.*

3. Research Methodology

3.1. Research Model

Based on the thirteen proposed hypotheses, the research model presented in Figure 1 illustrates how the propensity to trust, institution-based trust, perceived sensitivity of personal information and trusting beliefs in the mobile app affect the intention to use the mobile app. The propensity to trust is based on the individual's psychology. Most consumers do not approach a mobile app with a 'clean slate'; they have some existing beliefs. In this situation, as with others where risk is involved, the institutions play a role to ensure a process has the expected outcome. In addition to the individual psychology and the institutions that play a role, the mobile app itself inevitably plays a role and needs to be trusted. This complex model attempts to capture all of the most important dimensions of trust in this process rather than just a subsection of them.

3.2. Data Collection

A survey was implemented based on the research model and the thirteen hypotheses that were developed from the literature. Each question has a Likert scale with seven points, from strongly disagree (1) to strongly agree (7), for the participant to give their feedback. Relevant survey questions successfully used in the past were used as much as possible. Existing questions were adapted for (a) propensity to trust [11,15], (b) personal information privacy concern [42,43], (c) institution-based trust [15], (d) trusting beliefs in technology [11,19], and (e) intention to use a technology [15,44].

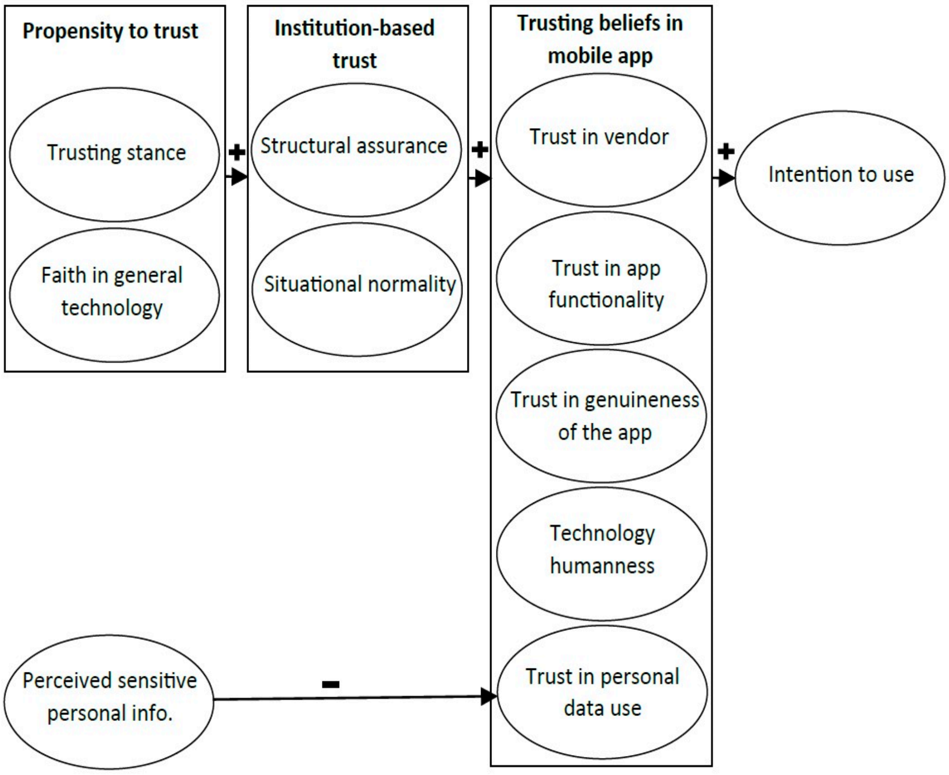
Propensity to trust
Trusting stance
Faith in general technology
Institution-based trust
Structural assurance
Situational normality
Trusting beliefs in mobile app
Trust in vendor
Trust in app functionality
Trust in genuineness of the app
Technology humanness
Trust in personal data use
Intention to use
Perceived sensitive personal info.
+
+
+
-

Figure 1. Consumer trust and privacy concerns in mobile apps with enhanced AI.

The survey questions were trialed with twelve participants to verify that they were clear, understandable, and would not encourage non-response bias. Based on the maximum number of arrows pointing at a construct being four, a statistical power of 80%, and a significance level of 1%, the minimum required sample was 191 [45]. The survey was offered to German residents through the SoSci Survey website, which fulfills GDPR requirements and stores the data within the EU. As a country's laws, regulation, and culture can influence consumers beliefs, a sample from one country was collected. The minimum age limit to participate was eighteen years old. Incomplete submissions and submissions that did not appear to be valid were taken out. Based on the percentage of surveys that started being completed and the low percentage of responses that were potentially completed intentionally wrong, such as by selecting the same answer to all the questions, there is no evidence of non-response bias. Given that the topic is neither controversial nor sensitive, it is not a typical case of non-response bias. The final sample consists of 317 participants. The sample collected is sufficiently balanced between men and women and across different age groups of adults, as shown in Table 2.

Table 2. Profile of the respondents.

Demographic Profile	Frequency	Percentage
Gender		
Male	176	55.5
Female	141	44.5
Age		
<18	0	0
18–30	144	45.4
31–40	115	36.3
41–50	33	10.4
51–60	14	4.4
>60	11	3.5

3.3. Data Analysis Method

The survey evaluated the validity and generalizability of the hypotheses [46]. The quantitative data were analyzed in a number of ways including descriptive analysis and Structural Equation Modeling, applying widely accepted procedures [47]. The quantitative analysis applied Partial Least Squares-Structural Equation Modeling (PLS-SEM) methods with the SmartPLS software. PLS-SEM is chosen because it can be applied to complex models with many variables and a relatively small sample. It is preferred over CB-SEM because it is better suited for exploring immature models, while CB-SEM is more focused on validating mature models [45]. The first stage of the analysis, the measurement model, tests the relationship between the latent variables and their respective measured variables. The second stage of the analysis, the structural model, tests the relationships between the latent variables.

4. Analysis and Results

4.1. Measurement Model

The measurement model is reflective, meaning that the arrows travel from the latent variable to the measured variables and not the other way around. Due to high collinearity, SA03 and TS01 were taken out of the dataset and not used in the modeling. The measurement model of the relationship between the observed and latent variable is evaluated in several ways, including the factor loading, composite reliability, discriminant validity and average variance extracted. As Table 3 shows, the factor loadings exceed 0.7, so the indicator reliability is sufficient [45]. Construct reliability is measured with the composite reliability (CR) and exceeds 0.7. Composite reliability evaluates the internal consistency of the indicator of a latent variable. Construct validity, how well indicators explain the latent variable, is measured by the convergent validity. The convergent validity is evaluated by the average variance extracted (AVE). The average variance extracted (AVE) exceeds 0.5 for the ten latent variables. The discriminant validity evaluated with the Fornell–Larcker criterion presented in Appendix A shows that the indicators are more closely correlated to their latent variable than others. The analysis shows strong support for the measurement model.

Table 3. Results of the evaluation of the measurement model.

Scale/Item	Loadings	CR	AVE
Trusting stance		0.899	0.908
TS01	0.953		
TS02	0.948		
Faith in general technology		0.955	0.876
FT01	0.946		
FT02	0.932		
FT03	0.929		
Perceived sensitivity of personal info.		0.942	0.890
PI01	0.951		
PI02	0.935		
Structural assurance		0.887	0.798
SA01	0.926		
SA02	0.877		
Situational normality		0.873	0.696
SN01	0.842		
SN02	0.822		
SN03	0.838		
Trust in vendor		0.872	0.696
TI01	0.930		
TI02	0.784		
TI03	0.780		

Table 3. *Cont.*

Scale/Item	Loadings	CR	AVE
Trust in app functionality		0.753	0.508
Video information, VI01	0.619		
Video information, VI02	0.664		
Free trial version, FTV01	0.836		
Trust in genuineness of app.		0.807	0.584
App platform prom., AP03	0.793		
App platform prom., AP04	0.823		
Clear and acc. descr., CA01	0.668		
Technology humanness		0.951	0.866
TH01	0.948		
TH02	0.911		
TH03	0.933		
Trust in personal data use		0.942	0.768
PH01	0.931		
PH02	0.817		
PF03	0.877		

4.2. Structural Model and Hypotheses Testing

The structural model of the relationship between the latent variables was measured in several ways. The effect sizes are from 0.016 to 0.832, as illustrated in Table 4. The path that measures hypothesis 4 has an effect of 0.016, which is below 0.02 and therefore can be considered to have no significant effect [48] despite being quite close. The paths that measure hypotheses 3, 6, 7 and 8 are between 0.02 and 0.15 and therefore have a weak but significant effect [48]. The paths that measure hypotheses 1, 9 and 12 are between 0.15 and 0.35 and therefore have a moderate effect. Lastly, the path that measures hypotheses 2, 5, 10, 11 and 13 are above 0.35 and show a strong effect [48]. Considering the complexity of the model and the number of variables when interpreting the results, there is support for the structural model and the hypotheses.

Table 4. Structural model effect size.

Path	Effect Size
H1: Trusting stance positively affects propensity to trust, (TS-PT)	0.222
H2: Faith in general technology positively affects propensity to trust, (FT-PT)	0.741
H3: Propensity to trust positively affects institution-based trust, (PT-IBT)	0.096
H4: Structural assurance in the internet positively affects institution-based trust, (SA-IBT)	0.016
H5: Situational normality positively affects trusting beliefs on institution-based trust, (SN-IBT)	0.822
H6: Institution-based trust positively affects trusting beliefs in a mob. app, (IBT-TB)	0.044
H7: Trust in the vendor positively affects trusting belief in a mob. app, (TI-TB)	0.098
H8: Trust in the reliability of the mob. app functionality positively affects trusting belief in a mob. app, (TIF-TB)	0.073
H9: Trust in the genuineness of the app positively affects trusting belief in a mob. app, (TG-TB)	0.246
H10: A technology that is perceived to have a higher humanness positively affects trusting belief in a mob. app, (TH-TB)	0.807
H11: A high perceived sensitivity of personal information negatively affects trust in personal data use, (PI-PH)	0.832
H12: Trust in the responsible use of personal data positively affects trusting belief in a mob. app, (PH-TBMA)	0.162
H13: Trusting belief in a mob. app. positively affects intention to use a mob. app, (TBMA-IU)	0.709

5. Discussion

5.1. Theoretical Implications

Trust and privacy concern have been explored in e-commerce, but the enhanced role of AI requires a re-evaluation of the consumer's perspective on these issues. Several studies are revisiting the role of trust in other contexts to update our understanding by incorporating recent developments [49–51]. This research identifies three main forms of trust in purchasing a mobile app. A model with fourteen variables is tested with the PLS-SEM method.

The strong support for the measurement model suggests that the latent variables of trust and privacy concern researched here can be measured accurately by the observed indicator variables used in this study. The large number of hypotheses tested in this research is necessary to cover the user's perspective comprehensively. The literature suggests that several variables influence trust and privacy concern in e-commerce and mobile commerce. Hypothesis 4, on the role of structural assurance of the internet on trust, does not have a significant effect despite being very close to the necessary threshold and is not supported by the analysis. The rest of the hypotheses have a significant effect and are supported.

Two of the hypotheses that have a lower effect are related to institutional trust. These are firstly the effect of propensity to trust on institution-based trust (H3) and secondly the effect of institution-based trust on trusting beliefs in a mobile app (H6). While the role of institutional trust in business-to-consumer (B2C) e-commerce has been supported in some contexts in the literature [52], in others, it has not been supported [53]. Several models of the consumer behavior in e-commerce trust do not include institutional trust. This research corroborates that institutional trust is not as significant as some other forms of trust. Two other variables with a lower effect are firstly trust in the vendor, which has a positive effect on the trusting belief in a mobile app (H7), and secondly trust in the reliability of the mobile app functionality, which has a positive effect on the trusting belief in a mobile app (H8).

The remaining nine hypotheses have a larger effect within the model. This includes the two variables that link privacy concern to trust. These are firstly that a high perceived sensitivity of personal information will have a negative effect on trust in personal data use (H11) and secondly that trust in the responsible use of personal data has a positive effect on the trusting belief in a mobile app (H12). Trust and privacy concern are usually found to be strongly linked [54] particularly when there are large volumes of information [55] or very sensitive information [16]. This research suggests purchasing a mobile app involves a similar relationship between trust and privacy. These findings reinforce the importance of finding new approaches to handling personal and sensitive information [56]. The other hypotheses with a strong effect within the model are trusting stance (H1), faith in general technology (H2), situational normality (H5), trust in the genuineness of the app (H9), humanness of the technology (H10) and trusting belief (H13).

5.2. Managerial Implications

This research has managerial implications for those selling mobile apps and other institutions, such as platforms hosting the apps and regulators. It also has implications for other parts of the value chain, such as those developing and providing the payment functionality used to purchase the app. A lesson that applies to all of these organizations is that they all have a role in building trust. If they all contribute to building trust, they will make each other's job easier.

Communicating to the consumer that the right steps are taken is a big part of building trust. Given that the consumer will only read a few lines of text, see a few images, and possibly watch a short video, the seller of the mobile app must be very concise and effective in covering all the identified areas to build trust. For example, measures must be in place to ensure the consumer's personal information is not leaked, and equally importantly, this must be communicated.

Mobile app providers have five clear areas to build trust: (a) trust in the vendor of a mobile app; (b) trust in the reliability of the mobile app functionality; (c) trust in the genuineness of the app; (d) have a higher humanness in the mobile app; (e) trust in the responsible use of personal data. The institutions involved, such as regulators, should build trust by reinforcing the stable and normal functioning of the internet. Any negative events related to the functioning of the internet and e-commerce, such as ransomware attacks, can reduce trust.

6. Conclusions and Future Work

While trust and privacy concern have been explored in e-commerce, the enhanced role of AI requires a re-evaluation and an attempt to holistically cover the consumer's perspective on these issues. The research on trust that created the models used today was developed when AI was less pervasive, and capable, than today. As these capabilities are increasing rapidly, the models of trust need to be re-evaluated regularly to see if, and how, they change.

In this research, the factors affecting the consumer's trust when purchasing a mobile app have been explored, and a research model has been developed and evaluated by empirical data collection and analysis. The increasing use of mobile devices by the consumer, and AI by private and public organizations, has created new challenges to developing strong trust. Furthermore, the increasing socialization of information systems elevates the influence of the humanness of the technology in relation to the technological functionality. For the increasing impact of these influences on trust to be evaluated, they need to be incorporated into existing models along more mature extensively validated influences.

Therefore, the constructs of perceived sensitivity of personal information, trust in personal data use and technology humanness were added to a model that already included the more mature constructs of trusting stance, faith in general technology, trust in vendor, app functionality and genuineness. The role of the vendor is also different in this context. These vendors are usually a small number of reputable online platforms from technology giants as opposed to being sold by the organization that creates the mobile app. The analysis indicates that the user's trust in an institution has a weaker relationship to their trust in the mobile app, but privacy concerns are strongly related to trust.

The findings of this research have practical implications primarily for developers of mobile apps, developers of the online platforms that offer them, developers of payment systems and those engaged in creating and utilizing big data and AI. These findings can stimulate further research into the user's perspective on trust and personal information privacy concerns. In particular, the reduced role of institutional trust and the elevated role of privacy concerns should be explored further. For example, other models of trust that include institutional trust can be re-evaluated to verify that they still have a significant effect on a consumer's trust in the current context where AI plays a larger role than in the past.

Author Contributions: Conceptualization, A.Z.; methodology, A.Z.; formal analysis, A.Z. and S.F.; investigation, A.Z. and S.F.; resources, A.Z. and S.F.; data curation, A.Z. and S.F.; writing—original draft preparation, A.Z. and S.F.; writing—review and editing, A.Z. and S.F.; visualization, A.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

Appendix A

Table A1. Discriminant validity: Fornell–Larcker criterion.

	FT	IBT	IU	PF	PI	PT	SA	SN	TA	TB	TG	TH	TI	TS
FT	0.936													
IBT	0.164	0.637												
IU	0.743	0.002	0.972											
PF	0.391	0.006	0.303	0.876										
PI	0.316	0.052	0.255	0.785	0.943									
PT	0.914	0.13	0.714	0.362	0.323	0.901								
SA	0.17	0.276	0.249	0.35	0.334	0.095	0.893							
SN	0.076	0.832	0.053	0.116	0.095	0.043	0.346	0.834						
TA	0.172	0.45	0.139	0.19	0.174	0.211	0.258	0.36	0.713					
TB	0.663	0.181	0.709	0.19	0.145	0.717	0.024	0.205	0.274	0.668				
TG	0.27	0.246	0.402	0.033	0.076	0.311	0.197	0.266	0.59	0.486	0.764			
TH	0.728	0.075	0.766	0.441	0.375	0.777	0.116	0.019	0.06	0.83	0.283	0.931		
TI	0.234	0.19	0.142	0.046	0.011	0.213	0.323	0.126	0.445	0.111	0.373	0.19	0.834	
TS	0.769	0.013	0.745	0.397	0.338	0.792	0.168	0.016	0.002	0.666	0.294	0.755	0.189	0.953

References

1. Trenz, M.; Veit, D.J.; Tan, C.-W. Disentangling the Impact of Omnichannel Integration on Consumer Behavior in Integrated Sales Channels. *MIS Q.* **2020**, *44*, 1207–1258. [CrossRef]
2. Liao, C.; To, P.-L.; Wong, Y.-C.; Palvia, P.; Kakhki, M.D. The Impact of Presentation Mode and Product Type on Online Impulse Buying Decisions. *J. Electron. Commer. Res.* **2016**, *17*, 153–168.
3. Preibusch, S.; Peetz, T.; Acar, G.; Berendt, B. Shopping for Privacy: Purchase Details Leaked to PayPal. *Electron. Commer. Res. Appl.* **2016**, *15*, 52–64. [CrossRef]
4. Teo, T.S.H.; Liu, J. Consumer Trust in E-Commerce in the United States, Singapore and China. *Omega* **2007**, *35*, 22–38. [CrossRef]
5. Venkatesh, V.; Thong, J.Y.L.; Xu, X. Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead. *J. Assoc. Inf. Syst.* **2016**, *17*, 328–376. [CrossRef]
6. Hengstler, M.; Enkel, E.; Duelli, S. Applied Artificial Intelligence and Trust—The Case of Autonomous Vehicles and Medical Assistance Devices. *Technol. Forecast. Soc. Change* **2016**, *105*, 105–120. [CrossRef]
7. Müller, R.; Andersen, E.S.; Kvalnes, Ø.; Shao, J.; Sankaran, S.; Turner, J.R.; Biesenthal, C.; Walker, D.; Gudergan, S. The Interrelationship of Governance, Trust, and Ethics in Temporary Organizations. *Proj. Manag. J.* **2013**, *44*, 26–44. [CrossRef]
8. Zarifis, A.; Efthymiou, L.; Cheng, X.; Demetriou, S. Consumer Trust in Digital Currency Enabled Transactions. *Lect. Notes Bus. Inf. Process.* **2014**, *183*, 307–317. [CrossRef]
9. Barth, S.; de Jong, M.D.T.; Junger, M.; Hartel, P.H.; Roppelt, J.C. Putting the Privacy Paradox to the Test: Online Privacy and Security Behaviors among Users with Technical Knowledge, Privacy Awareness, and Financial Resources. *Telemat. Inform.* **2019**, *41*, 55–69. [CrossRef]
10. Canhoto, A.I.; Keegan, B.J.; Ryzhikh, M. Snakes and Ladders: Unpacking the Personalisation-Privacy Paradox in the Context of AI-Enabled Personalisation in the Physical Retail Environment. *Inf. Syst. Front.* **2023**. [CrossRef]
11. McKnight, H.; Carter, M.; Thatcher, J.B.; Clay, P. Trust in a Specific Technology: An Investigation of Its Components and Measures. *ACM Trans. Manag. Inf. Syst.* **2011**, *2*, 1–25. [CrossRef]
12. Molina-Coronado, B.; Mori, U.; Mendiburu, A.; Miguel-Alonso, J. Towards a fair comparison and realistic evaluation framework of android malware detectors based on static analysis and machine learning. *Comput. Secur.* **2023**, *124*, 102996. [CrossRef]
13. Zhu, H.; Wei, H.; Wang, L.; Xu, Z.; Sheng, V.S. An effective end-to-end android malware detection method. *Expert Syst. Appl.* **2023**, *218*, 119593. [CrossRef]
14. Rodrigues, V.F.; Policarpo, L.M.; da Silveira, D.E.; da Rosa Righi, R.; da Costa, C.A.; Barbosa, J.L.V.; Antunes, R.S.; Scorsatto, R.; Arcot, T. Fraud detection and prevention in e-commerce: A systematic literature review. *Electron. Commer. Res. Appl.* **2022**, *56*, 101207. [CrossRef]
15. Kim, K.K.; Prabhakar, B. Initial Trust and the Adoption of B2C E-Commerce. *ACM SIGMIS Database* **2004**, *35*, 50–64. [CrossRef]
16. Bansal, G.; Zahedi, F.M.; Gefen, D. The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online. *Decis. Support Syst.* **2010**, *49*, 138–150. [CrossRef]
17. Vance, A.; Elie-Dit-Cosaque, C.; Straub, D.W. Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture. *J. Manag. Inf. Syst.* **2008**, *24*, 73–100. [CrossRef]
18. Zhang, Z.; Gu, C. Effects of Consumer Social Interaction on Trust in Online Group-Buying Contexts: An Empirical Study in China. *J. Electron. Commer. Res.* **2015**, *16*, 1–21.
19. Lankton, N.; McKnight, H.; Tripp, J. Technology, Humanness, and Trust: Rethinking Trust in Technology. *J. Assoc. Inf. Technol.* **2015**, *16*, 880–918. [CrossRef]

20. Degutis, M.; Urbonavičius, S.; Hollebeek, L.D.; Anselmsson, J. Consumers' willingness to disclose their personal data in e-commerce: A reciprocity-based social exchange perspective. *J. Retail. Consum. Serv.* **2023**, *74*, 103385. [CrossRef]
21. Pang, H.; Ruan, Y. Can information and communication overload influence smartphone app users' social network exhaustion, privacy invasion and discontinuance intention? A cognition-affect-conation approach. *J. Retail. Consum. Serv.* **2023**, *73*, 103378. [CrossRef]
22. McKnight, H.; Choudhury, V.; Kacmar, C. Developing and Validating Trust Measures for E-Commerce: An Integrative Typology. *Inf. Syst. Res.* **2002**, *13*, 334–359. [CrossRef]
23. Sha, W. Types of Structural Assurance and Their Relationships with Trusting Intentions in Business-to-Consumer e-Commerce. *Electron. Mark.* **2009**, *19*, 43–54. [CrossRef]
24. Bambauer-Sachse, S.; Mangold, S. Do Consumers Still Believe What Is Said in Online Product Reviews? A Persuasion Knowledge Approach. *J. Retail. Consum. Serv.* **2013**, *20*, 373–381. [CrossRef]
25. Sridhar, S.; Srinivasan, R. Social Influence Effects in Online Product Ratings. *J. Mark.* **2012**, *76*, 70–88. [CrossRef]
26. Hu, N.; Koh, N.S.; Reddy, S.K. Ratings Lead You to the Product, Reviews Help You Clinch It? The Mediating Role of Online Review Sentiments on Product Sales. *Decis. Support Syst.* **2014**, *57*, 42–53. [CrossRef]
27. Metzger, M.J. Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure. *Commun. Res.* **2006**, *33*, 155–179. [CrossRef]
28. Einwiller, S. When Reputation Engenders Trust: An Empirical Investigation in Business-to-Consumer Electronic Commerce. *Electron. Mark.* **2003**, *13*, 196–209. [CrossRef]
29. Yoo, J.; Kim, M. The Effects of Online Product Presentation on Consumer Responses: A Mental Imagery Perspective. *J. Bus. Res.* **2014**, *67*, 2464–2472. [CrossRef]
30. Li, M.; Wei, K.-K.; Tayi, G.K.; Tan, C.-H. The Moderating Role of Information Load on Online Product Presentation. *Inf. Manag.* **2016**, *53*, 467–480. [CrossRef]
31. Wang, T.; Oh, L.-B.; Wang, K.; Yuan, Y. User Adoption and Purchasing Intention after Free Trial: An Empirical Study of Mobile Newspapers. *Inf. Syst. E-Bus. Manag.* **2013**, *11*, 189–210. [CrossRef]
32. Tang, Q.C. Free Trial or No Free Trial: Optimal Software Product Design with Network Externalities. *Am. Conf. Inf. Syst.* **2003**, *459*, 3417–3419. [CrossRef]
33. Wagner, T.M.; Benlian, A.; Hess, T. Converting Freemium Customers from Free to Premium: The Role of the Perceived Premium Fit in the Case of Music as a Service. *Electron. Mark.* **2014**, *24*, 259–268. [CrossRef]
34. Cheng, H.K.; Liu, Y. Optimal Software Free Trial Strategy: The Impact of Network Externalities and Consumer Uncertainty. *Inf. Syst. Res.* **2012**, *23*, 488–504. [CrossRef]
35. Bocereg, A.; Gosa, R.; Endre-Laszlo, A.; Baciu, A.; Stahie, S. Real-Time Behavior-Based Detection on Android Reveals Dozens of Malicious Apps on Google Play Store. Available online: https://www.bitdefender.com/blog/labs/real-time-behavior-based-detection-on-android-reveal-dozens-of-malicious-apps-on-google-play-store/ (accessed on 13 September 2023).
36. Pavlou, P.A. Integrating Trust in Electronic Commerce with the Technology Acceptance Model: Model Development and Validation. *AMCIS* **2001**, *159*, 816–822.
37. Bardhan, I.; Chen, H.; Karahanna, E. Connecting Systems, Data, and People: A Multidisciplinary Research Roadmap for Chronic Disease Management. *MIS Q.* **2020**, *44*, 185–200.
38. Kreuter, F.; Haas, G.C.; Keusch, F.; Bähr, S.; Trappmann, M. Collecting Survey and Smartphone Sensor Data with an App: Opportunities and Challenges Around Privacy and Informed Consent. *Soc. Sci. Comput. Rev.* **2020**, *38*, 533–549. [CrossRef]
39. Bähr, S.; Haas, G.C.; Keusch, F.; Kreuter, F.; Trappmann, M. Missing Data and Other Measurement Quality Issues in Mobile Geolocation Sensor Data. *Soc. Sci. Comput. Rev.* **2020**, *40*, 212–235. [CrossRef]
40. Fishbein, M.; Ajzen, I. *Predicting and Changing Behavior: The Reasoned Action Approach*; Psychology Press: New York, NY, USA, 2010.
41. Venkatesh, V.; Davis, F.D. A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Manag. Sci.* **2000**, *46*, 186–204. [CrossRef]
42. Dinev, T.; Xu, H.; Smith, J.H.; Hart, P. Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *Eur. J. Inf. Syst.* **2013**, *22*, 295–316. [CrossRef]
43. Yun, H.; Lee, G.; Kim, D.J. A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Inf. Manag.* **2019**, *56*, 570–601. [CrossRef]
44. Venkatesh, V.; Morris, M.G.; Davis, G.B.; Davis, F.D. User Acceptance of Information Technology: Toward a unified view. *MIS Q.* **2003**, *27*, 425–478. [CrossRef]
45. Hair, J.; Hult, T.; Ringle, C.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 3rd ed.; Sage Publishing: Thousand Oaks, CA, USA, 2021.
46. Johnson, R.B.; Onwuegbuzie, A. Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educ. Res.* **2004**, *33*, 14–26. [CrossRef]
47. Gefen, D.; Rigdon, E.E.; Straub, D. An Update and Extension to SEM Guidelines for Administrative and Social Science Research. *MIS Q.* **2011**, *35*, iii-A7. [CrossRef]
48. Chin, W.W. The Partial Least Squares Approach to Structural Equation Modelling. In *Modern Methods for Business Research*; Marcoulides, G.A., Ed.; Lawrence Erlbaum Associates: Mahwah, NJ, USA, 1998; pp. 295–336.

49. Hamid, S.; Azhar, M. Behavioral Intention to Order Food and Beverage Items Using E-Commerce during COVID-19: An Integration of Theory of Planned Behavior (TPB) with Trust. *Br. Food J.* **2023**, *125*, 112–131. [CrossRef]
50. Wu, Y.; Huang, H. Influence of Perceived Value on Consumers' Continuous Purchase Intention in Live-Streaming E-Commerce—Mediated by Consumer Trust. *Sustainability* **2023**, *15*, 4432. [CrossRef]
51. Sun, Y.; Huang, Y.; Fang, X.; Yan, F. The Purchase Intention for Agricultural Products of Regional Public Brands: Examining the Influences of Awareness, Perceived Quality, and Brand Trust. *Math. Probl. Eng.* **2022**, *2022*, 4991059. [CrossRef]
52. Patnasingham, P.; Gefen, D.; Pavlou, P.A. The Role of Facilitating Conditions and Institutional Trust in Electronic Markets. *J. Electron. Commer. Organ.* **2005**, *14*, 69–82. [CrossRef]
53. Oliveira, T.; Alhinho, M.; Rita, P.; Dhillon, G. Modelling and Testing Consumer Trust Dimensions in E-Commerce. *Comput. Hum. Behav.* **2017**, *71*, 153–164. [CrossRef]
54. Saeed, S. A Customer-Centric View of E-Commerce Security and Privacy. *Appl. Sci.* **2023**, *13*, 1020. [CrossRef]
55. Saffarizadeh, K.; Boodraj, M.; Alashoor, T.M. Conversational Assistants: Investigating Privacy Concerns, Trust, and Self-Disclosure. In Proceedings of the International Conference on Information Systems (ICIS), Seoul, Republic of Korea, 10–13 December 2017.
56. Zhu, P.; Hu, J.; Li, X.; Zhu, Q. Using Blockchain Technology to Enhance the Traceability of Original Achievements. *IEEE Trans. Eng. Manag.* **2021**, *70*, 1693–1707. [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.