information

MDPI

Article

# What Drives Authorization in Mobile Applications? A Perspective of Privacy Boundary Management

**Jie Tang [1], Bin Zhang [1] and Umair Akram [2,*]**

[1] School of Economics and Management, Beijing University of Posts and Telecommunications,
Beijing 100876, China; jietang@bupt.edu.cn (J.T.); binzhang@bupt.edu.cn (B.Z.)
[2] School of Management, Jiangsu University, Zhenjiang 212013, China
* Correspondence: akram.umair88@gmail.com

**Abstract:** Personal information has been likened to "golden data", which companies have chased using every means possible. Via mobile apps, the incidents of compulsory authorization and excessive data collection have evoked privacy concerns and strong repercussions among app users. This manuscript proposes a privacy boundary management model, which elaborates how such users can demarcate and regulate their privacy boundaries. The survey data came from 453 users who authorized certain operations through mobile apps. The partial least squares (PLS) analysis method was used to validate the instrument and the proposed model. Results indicate that information relevance and transparency play a significant role in shaping app users' control–risk perceptions, while government regulation is more effective than industry self-discipline in promoting the formation of privacy boundaries. Unsurprisingly, privacy risk control perceptions significantly affect users' privacy concerns and trust beliefs, which are two vital factors that ultimately influence their willingness to authorize. The implications of conducting a thorough inquiry into app users' willingness to authorize their privacy information are far-reaching. In relation to this, app vendors should probe into the privacy-relevant beliefs of their users and enact effective privacy practices to intercept the economic and reputational damages induced by improper information collection. More significantly, a comprehensive understanding of users' willingness to authorize their information can serve as an essential reference for relevant regulatory bodies to formulate reasonable privacy protection policies in the future.

**Keywords:** communication privacy management; institutional privacy assurance; fair information practices; mobile application; authorizing intention

check for updates

**Citation:** Tang, J.; Zhang, B.; Akram, U. What Drives Authorization in Mobile Applications? A Perspective of Privacy Boundary Management. *Information* **2021**, *12*, 311. https://doi.org/10.3390/info12080311

Academic Editor: Maria Carmen Carnero

Received: 22 June 2021
Accepted: 27 July 2021
Published: 30 July 2021

## 1. Introduction

Mobile application (app) authorization refers to the process by which users give applications permission to gain back-end access to their relevant personal data or information in exchange for specialized functions and services in the mobile environment [1]. Paradoxically, authorization involves a ubiquitous game for almost all users, that is, personal information disclosure can lead to incredible experience and services [2], whereas incautious authorization will expose them to privacy threats and security pitfalls. Nowadays, the occurrence of pernicious incidents, such as personal information being illegally stored, shared, tampered with and exploited, aggravates the privacy concerns raised by certain groups [3–5]. Due to escalated concerns in online privacy, many mobile users now refuse to authorize the disclosure of personal information or simply falsify the actual data they share [6]. Such routinized privacy issues have morphed into one of the major obstacles to facilitate the healthy and orderly development of the mobile app industry.

A comprehensive understanding of users' privacy concerns and privacy decisions has always been a significant topic among information system (IS) studies. Communication privacy management (CPM) theory provides an effective framework for individual privacy decision-making [7]. To date, although it has been extensively adopted in the study of privacy management, only a few scholars have applied this theory into the mobile app context. Additionally, research on users' privacy decision-making has overwhelmingly focused on an individual level, including personality traits [8,9], prior experiences [10] and privacy perceptions [11] of information subjects, but how their privacy decision may be influenced by institutional privacy assurance mechanisms has rarely been discussed. Therefore, it is a matter of great concern, as well as a cut-in point of this study, to reduce the perception of uncertainty in user privacy decisions from the level of institutional guarantee and enhance the trust belief, so as to facilitate user authorizing intention.

Mobile devices are more likely to infringe users' privacy than other digital devices. Hence, depending on the conclusion of traditional Internet privacy research to comprehend users' privacy decision-making in the mobile context is far from enough [12]. Combined with the aforementioned research gaps and the mobile app context, the research objectives of this paper are mainly reflected in two aspects. First, we aim to gain a profound understanding of the dynamic process of mobile app users' authorizing decisions and to determine the salient determinants of their authorizing intention through an integrated model. The second goal is to excavate the impact of institutional privacy assurance mechanisms and fair information practice principles on users' perceptions of privacy and willingness to authorize. Drawing on the CPM theory as the main framework, we take the two institutional guarantee mechanisms of government regulation and industry self-discipline, and the two pivotal fair information practices principles of information relevance and information transparency, as the antecedent constructs of this study. Meanwhile, through the interaction of perceived privacy risk and perceived privacy control, privacy concern and trust, this paper jointly explores app users' authorization intentions and decision-making processes.

The theoretical and practical relevance of this study is of vital importance. We built a privacy decision model that integrates multiple theories, which can effectively demonstrate and analyze the direct and indirect factors that affect users' privacy disclosure intentions. Additionally, app providers will gain sufficient insights into the mechanisms behind users' information authorization through this analysis, which also provides important references as their privacy management or marketing behaviors. What is more, it will give enlightenment to the government and industry regulators to formulate more complete personal privacy protection laws and regulations, take the necessary data security tests and certifications, and then promote the healthy development of the app industry.

## 2. Theoretical Background

### *2.1. Communication Privacy Management*

The communication privacy management (CPM) theory, first proposed by Petronio [7], argues that if data subjects disclosed their private information to other recipients, the recipients become the co-owners of such information. These co-owners, however, may take liberties with the information; hence, coordinating ownership boundaries to collectively control the information is indispensable for the owners. Eventually, to determine what, when, and with whom the information can be shared, the two parties attain a set of access and protection rules through negotiation [13,14]. Following the essential viewpoints of Petronio [7], Child et al. [15] as well as Chang et al. [16], CPM theory can be extracted from three central elements: privacy ownership, privacy control, and privacy turbulence. Privacy management is the dynamic process of an individual opening or closing his/her privacy boundary to others. Information subjects and recipients initially demarcate privacy boundaries, experience boundary self-regulation, and ultimately reach a consensus on privacy decisions in the midst of privacy boundary coordination and turbulence.

The current study is specifically guided by the classic research of Xu et al. [17] and Widjaja et al. [18], in which boundary coordination and boundary turbulence are represented by fair information practices (FIP) and institutional privacy assurance (IPA). Meanwhile, to avert personal information that has been infringed upon effectually, Xu et al. [19]

elaborated that users' control and risk perceptions determine the bilateral privacy boundary. Once the risk-control assessment is completed, the individual's privacy boundary rules are temporarily formed. However, privacy boundaries are subject to constant variation and would be reshaped in subsequent interaction practices. Chang et al. [16] integrated the two privacy attitude factors of privacy concern and trust belief into their theoretical model to better explain the process of boundary self-regulation. When privacy boundaries achieve the best balance point through self-regulation, information subjects would make decisions in light of the privacy boundaries of both parties, i.e., clarifying the scope, time interval, and manner of information authorization.

### *2.2. Fair Information Practices*

The exchange of personal information is governed by the fairness of the social contract, which is essentially a commutation of promises [20,21]. Prior to information disclosure, consumers will evaluate the benefits against the costs of this operation. Once their perceived benefits outweigh the costs, they will autonomously engage in a social contract [22]. This social contract requires a mutual agreement on the fairness of the exchange, i.e., the FIP principle, which emphasizes that the sharing or disclosure of consumers' personal information is built upon a fair social contract, with the goal of enabling consumers to exercise sufficient control over the disclosure [23]. Some studies have proven that the implementation of FIP principles mitigates consumers' risk perceptions during the data disclosure. The gradual standardization of information collection in the mobile app industry is accompanied by the majority of app providers specifying individuals' privacy management through privacy policies. Hence, fairness and effectiveness of the privacy policy determine the outcome of the privacy risk control assessment.

### *2.3. Institutional Privacy Assurance*

Privacy research is not just limited to the category of self-protection, it is also a matter of what society deems appropriate to protect [24]. Culnan and Bies [20] and Xu et al. [19] summarized three primary approaches to protect user privacy protection: individual self-protection, industry self-discipline, and government regulation. These approaches are also differentiated into two broad categories based on their control agency, that is, individual control mechanism and proxy control mechanism. As the name implies, individual control means that the "self" acts as the control agent to protect personal privacy or information. In comparison, the proxy control mechanism refers to an institution-based approach in conjunction with some formidable external forces, such as ministries and trade associations, to enable consumers to greater control their personal information [17].

Among them, the conclusion that the perceived effectiveness of government regulation has a significant impact on enhancing users' perception of privacy control has been validated in numerous privacy studies, although some researchers continue to hold a skeptical attitude towards the availability of industry self-discipline for protecting personal information privacy [18,25,26]. Hence, privacy advocates have appealed for strengthening government regulations to guard against abuses of personal information by organizations or firms [20,27]. Nowadays, however, industry associations and third-party institutions that protect personal information also play an increasingly crucial role in regulating enterprise behavior and protecting the legitimate rights and interests of users. Based on the current situation, our research focuses on the reciprocal effects of the two constructs on individuals' privacy perceptions.

## **3. Research Model and Hypotheses**

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation, as well as the experimental conclusions that can be drawn.

### 3.1. Effects of Boundary Coordination on Boundary Rule Formation

The fairness and effectiveness of the rules serve as the basis for the formation of privacy boundaries [28]. In the study of privacy disclosure among e-commerce consumers, Li et al. [22] examined the degree of fair practice by characterizing the relevance and clarity of data obtained by firms. Meanwhile, the General Data Protection Regulations (GDPR) stipulate that the data processing conducted by the data controller or processor must follow the principles of accuracy, necessity, and timeliness as well as take relevancy and necessity as the limit. Accordingly, we take the two constructs of information relevance and awareness as the evaluation indexes to gauge the fairness and effectiveness of app users' authorized applications.

#### 3.1.1. Information Relevance and Control-Risk Perceptions

Relevance is a crucial information feature, and its identification involves the psychological assessment process initiated by users to assess the extent to which external resources can meet their personal needs, goals, and values [29]. It is a multi-dimensional cognitive concept whose meaning hinges on people's cognition of the usefulness, value, or utility of a problem or task at hand [30]. Xu and Chen [30] proposed the following criteria that users should adopt when making relevance judgment: timeliness, novelty, reliability, and intelligibility. In the context of mobile apps, sometimes users cannot judge only from the permission itself, so specific decision situations need to be combined. We assume that the relevance of authorized information mainly reflects the degree of relevance between the personal information collected by mobile apps and the permission to request access and the core functions provided by mobile apps.

When studying the concept of organizational justice, Stanton and Stam [31] observed that the privacy boundary between organizations and individuals is affected by the correlation between information requests and tasks. Additionally, Zimmer et al. [32] found that the risk perception of users is considerably weakened if the information provided by consumers is legitimate or useful for the functional services of the website. Li et al. [22] regarded the relevance of user information collected by online websites as fairness levers. They believed that if the information collected by online websites was not relevant to online transactions, even the low-risk information collected, it would trigger their awareness of privacy protection and increase their perception and concern about privacy risks. Based on this notion, the current paper proposes the following hypotheses:

**Hypothesis 1 (H1).** *The relevance of authorized information is positively related to the perceived privacy control of mobile app users.*

**Hypothesis 2 (H2).** *The relevance of authorized information is negatively related to the perceived privacy risk of mobile app users.*

#### 3.1.2. Information Transparency and Control-Risk Perception

Information transparency is a "reasonable expectation of privacy" [33]. In the mobile app market, the clarity of authorized information is mostly reflected through the privacy policies provided by app providers. Consequently, we define information transparency as the privacy policies or other specifications that could clearly communicate to users regarding their data collection and processing. Many previous studies have demonstrated the significant impacts of information transparency on privacy risks. Milne and Culnan [34], for example, believed that the clarity of privacy clauses can improve the transparency of information collection process, thus reducing consumers' perceived risk of disclosing their personal information online. Li et al. [22] confirmed that consumers tend to have a stronger sense of control over privacy and a lower belief in perceived privacy risks when they perceive that the privacy policy of websites is concise, clear, and understandable. Zhou et al. [35] clarified that, during B2C e-commerce website transactions, the transparency of information could reduce consumers' risk perception and improve their purchase intention. It has been proven that, if the privacy policy specifies what information is collected and whether and how the collected information is used for other purposes, the users' perceived risks will be reduced, and their sense of privacy control will be enhanced [36]. Accordingly, we propose the following hypotheses:

**Hypothesis 3 (H3).** *The transparency of authorized information is positively related to the perceived privacy control of mobile app users.*

**Hypothesis 4 (H4).** *The transparency of authorized information is negatively related to the perceived privacy risk of mobile app users.*

### *3.2. Effects of Boundary Turbulence on Boundary Rule Formation*

Due to the complexity of boundary coordination, when there is information intrusion from outside or when the boundary coordination mechanism no longer functions, the privacy boundary fluctuates [7,17]. Once boundary shock occurs, individuals will seek a third party to defend their rights and interests by seeking institutional guarantees, such as government laws, regulations, and industry standards [17]. Institutional guarantee is an intervention measure to protect users' personal information at the macro and industry levels. In the context of mobile apps, we divided the institutional guarantee into two parts: government regulation and industry self-discipline, and both are considered crucial factors affecting users' control–risk perceptions.

#### 3.2.1. Government Regulation and Control-Risk Perceptions

The use of government regulations, which is a common approach in recent privacy studies [19,37], symbolizes a strong institutional structural guarantee provided by the judicial and legislative branches of a government [38,39]. In the current article, these refer to the relevant laws and regulations that guarantee the protection of users' privacy and personal information. Examples are the fair information practice law (FIPPS) in the United States, which embodies the protective principle of personal information and the general data protection regulation (GDPR) issued by the European Union in 2015. In China, although there is currently no unified law analogous to GDPR, the relevant provisions on personal information protection are scattered in several legal documents.

According to Spiro and Houghteling [40], legal institutions are the most powerful methods of enforcing agency control and can be used to deter unlawful conduct by threatening severe penalties, if necessary, to maintain its deterrent effect. Xu et al. [19] concluded that, in the process of forming privacy boundaries, government regulations serve as an important reference for consumers, positively influencing their perceived privacy control and appropriately eliminating their risk perceptions. Hence, we reckon that in a favorable regulatory environment, comparatively perfect information security and privacy legislation will enhance the user's ability to control authorized personal information, thus reducing the uncertainty and risk of disclosure. Based on this idea, the following hypothesis are proposed:

**Hypothesis 5 (H5).** *Government regulations are positively related to the perceived privacy control of mobile app users.*

**Hypothesis 6 (H6).** *Government regulations are negatively related to the perceived privacy risk of mobile app users.*

#### 3.2.2. Industry Self-Discipline and Control-Risk Perceptions

Industry self-regulation is a series of mutual restraint and self-management activities executed by industry stakeholders to supplement government regulation and promote the development of industry norms. This is usually carried out by certain organizations, such as industry alliances, trade associations, or third-party certification bodies, and is considered an effective means of protecting user privacy. In practice, the formation of self-regulatory associations (e.g., direct marketing associations), the promulgation of regulations or codes, and the use of third-party assessments or certifications (e.g., TRUSTe) can all provide assurance that the industry, as a whole, is exerting efforts to protect personal information while also increasing the perception of privacy protection among individuals [20].

The United States Wireless Telecommunications and Internet Association (CTIA), which has developed guidelines for LBS providers in handling location-related personal information, is a prime example of an industry self-regulatory body [41]. Meanwhile, many websites have attempted to enhance website security by establishing relationships with third-party assurance bodies. One example is TRUSTe, which is a third-party certification agency that has provided professional privacy certification services for many enterprises, as well as detailed privacy practices and implementation guidelines for different industries, thus ensuring the development of industry norms and the rational use of users' private information.

Xu et al. [19] argued that the establishment of self-protection associations or certification mechanisms in the industry can promote users' sense of control over their personal information. Additionally, Kim et al. [42] substantiated that the assurance seals have a dominant effect on online shopping website consumers' perceived risks. In the context of mobile apps, we believe that the establishment of an industry alliance, the launch of alliance standard policies, and the implementation of third-party security authentication in the industry are all indispensable measures to protect the security of users' personal information and enhance the practice of user privacy at the industry level. Therefore, this paper proposes the following hypotheses:

**Hypothesis 7 (H7).** *Industry self-discipline is positively related to the perceived privacy control of mobile app users.*

**Hypothesis 8 (H8).** *Industry self-discipline is negatively related to the perceived privacy risk of mobile app users.*

### *3.3. Effects of Boundary Rule Formation on Boundary Self-Regulation*

In CPM theory, knowing how individuals view privacy issues is crucial in determining how they establish their privacy boundaries with the outside world [7,43,44]. In accordance with Chang et al. [16], who studied privacy management, we consider that app users' perceived privacy control and perceived privacy risk are critical factors that affect the formation of their privacy boundaries with the other parts.

#### 3.3.1. Perceived Privacy Control and Privacy Concern, Trust

In different studies, the connotation of privacy control has been interpreted diversely. For example, Malhotra et al. [21] regarded privacy control as the right of consumers to challenge, select, and waive an organizational practice to direct or influence organizational privacy compliance. Xu and Teo [45] argued that privacy control is related but independent of privacy concerns; they also explored the nature of control against the backdrop of privacy from the psychology perspective. In this current paper, we defined perceived privacy control as an app users' belief in grasping and controlling the release and dissemination of their own private information; that is, a belief in their ability to manage their authorized personal information.

Enhancing users' control perception is one of the approaches to alleviate their privacy concerns and enhance their trust belief. According to Hajli and Lin [46], SNS users' sense of control over information reduces their privacy concerns. Taddei and Contena [47] pointed out that when users perceive that they can fully control their personal information, a higher degree of trust in information collectors or users would be established. Krasnova et al. [48] and Libaque-Sáenz et al. [36] also confirmed the perceived privacy control of OSN and mobile app users' negative relationship with perceived privacy risk. Aiming at the real circumstance of our studies, we proposed the following hypotheses:

**Hypothesis 9 (H9).** *Perceived privacy control is negatively related to the privacy concern of mobile app users.*

**Hypothesis 10 (H10).** *Perceived privacy control is positively related to the trust level of mobile app users.*

**Hypothesis 11 (H11).** *Perceived privacy control is negatively related to the perceived privacy risk of mobile app users.*

#### 3.3.2. Perceived Privacy Risk and Privacy Concern, Trust

Risk is defined as "the uncertainty caused by potential negative results and [the] other party's opportunistic behaviors" [49]. In electronic services, users must submit their personal information before accepting functional services. With the users' privacy information being collected, processed, disseminated, and invaded, they will generate the privacy risk perception consciously and unconsciously. Shaw and Sergueeva [50] and Xu et al. [9] identified perceived privacy risk as an important subset of the formation of privacy boundaries and a pivotal component of the cost–benefit assessment. In the context of mobile app authorization, perceived privacy risk is defined as app users' expectation of loss related to personal information authorization. Early studies have suggested that when a threatening situation is apparent, users' concerns about privacy increased significantly [51,52]. Additionally, Liu et al. [53] and Kim and Koo [54] have investigated the interaction of trust and risk belief, revealing that users' perceived privacy risk negatively influenced their trust in electronic services. In the current work, we believe that the higher a person's perception of privacy risks is, the more concerned he/she will be about the future employment of this information, and the less trust he/she will have in authorized app providers. Thus, we propose the following hypotheses:

**Hypothesis 12 (H12).** *Perceived privacy risk is positively related to the privacy concern of mobile app users.*

**Hypothesis 13 (H13).** *Perceived privacy risk is negatively related to the trust of mobile app users.*

### *3.4. Effects of Boundary Self-Regulation on Boundary Decision*

Privacy concerns and trust are two common proxies of attitudinal factors studied in user privacy research [55,56]. These reflect people's mental states towards privacy issues [49]. Both the theory of reasoned action (TRA) and theory of planned behavior (TPB) models highlight the influence of beliefs on behavior. Dinev and Hart [52] argued that the decision-making process of personal privacy disclosure may be jointly determined by two opposing beliefs, namely, trust and privacy concern. Privacy concern represents a negative psychological state, and trust is a positive psychological state that affects the overall self-assessed state of perceived privacy [57].

#### 3.4.1. Privacy Concern and Intention to Authorize Personal Information

Information privacy concern (hereafter referred to as "privacy concern")—a fundamental concept in IS research—is originally defined in the literature as employees' inherent misgivings about possible loss of privacy in organizational practices [17]. Dinev and Hart [44] regarded privacy concern as the internalization of users' risk beliefs, which can be derived from their assessment of the risks associated with personal information disclosure. Additionally, the literature on information privacy defines privacy concern as a cognitive result of users weighing the pros and cons of privacy disclosure [58,59].

As mobile users are up against a set of serious privacy risks, especially in the authorization stages, this makes the privacy decision-making process more intricate. In exchange for service availability, users must share their privacy information, which can be abused by the app providers or other parties [60,61]. In this paper, we evaluate app users' concerns about their privacy in terms of excessive requests for individual permission, inappropriate use, and disclosure. Previous research has shown that users' continued growth in privacy concern may lead them to take additional privacy measures, such as withholding or falsifying personal information, using privacy-enhancing technologies (e.g., encryption), or requesting to be removed from mailing lists. By extension, there are studies that specifically examine the relationship between privacy concern and intention behaviors. Junglas et al. [62], Bansal et al. [63] and Degirmenci [64] all confirmed that privacy concern reduces users' willingness to disclose information. Meanwhile, Van Dyke et al. [65] have demonstrated that concern perception is the key influencer of mobile app users' trust. Hence, we present the following hypotheses:

**Hypothesis 14 (H14).** *Privacy concern is negatively related to the authorizing intention of mobile app users.*

**Hypothesis 15 (H15).** *Privacy concern is negatively related to the trust of mobile app users.*

### 3.4.2. Trust and Intention to Authorize Personal Information

Trust and trust-building mechanisms are crucial in mobile commerce on account of relieving uncertainty and risk in anonymous online communication and facilitating consumers' decision-making behaviors, such as personal information exchange and commodity transaction [66]. In the research on information disclosure, Malhotra et al. [21] defined trust belief as the extent to which organizations are deemed reliable in protecting users' personal information. Many studies on information systems, e-commerce, and mobile commerce have long substantiated individual trust as a strong predictor of users' behavioral decisions, highlighting the importance of trust in information sharing and personal information disclosure [63,67]. For instance, Schoenbachler and Gordon [68] and Wu et al. [69] argued that consumers typically weigh the risk of information privacy abuse or data breach when engaging in online activities; thus, they must develop trust in websites before disclosing information. In this paper, we define trust as the positive expectation of mobile app users on the possible loss of authorized personal information. This is jointly influenced by users' risk-control perception and concern regarding information security and privacy. Additionally, we proposed its positive effect on users' authorization willingness. Therefore, this study posits the following hypothesis:

**Hypothesis 16 (H16).** *Trust is positively related to the authorizing intention of mobile app users.*

Figure 1 presents the research model.

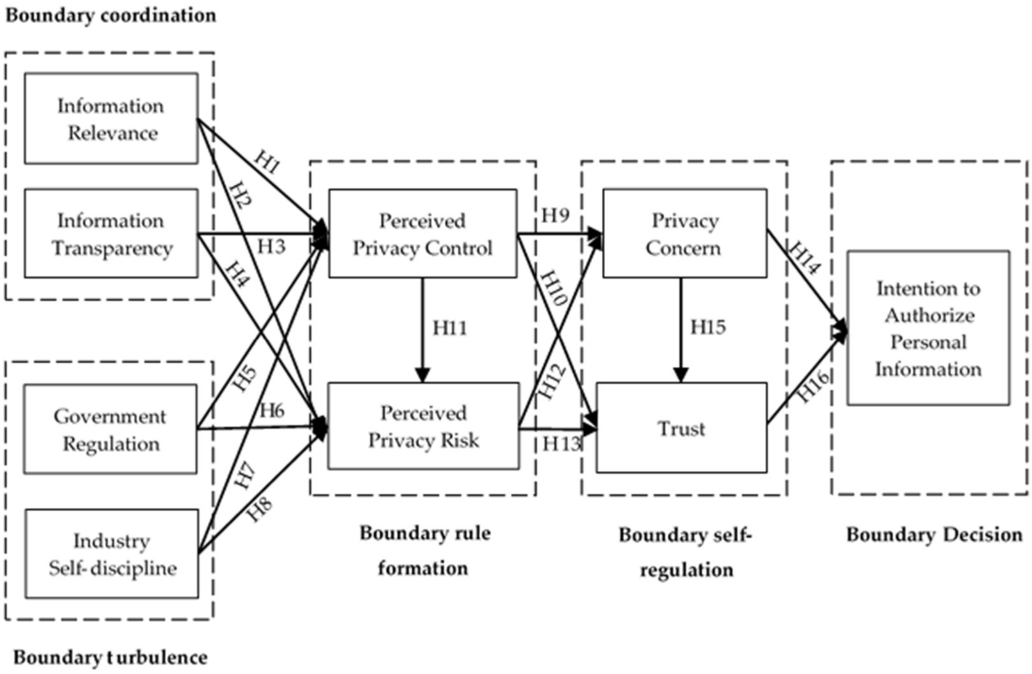

**Figure 1.** Conceptual model.

## 4. Methodology

### *4.1. Measurement Development*

Our empirical strategy was to use a scenario-based questionnaire in which the subjects are placed in a hypothetical scenario and their responses were collected [70]. All variables were derived from previous studies, and some measurement items were slightly modified to fit the context of privacy authorization in mobile apps. A total of 15 hypothesis tests and 29 measures were formed. We measured the items by a seven-point Likert scale, from low to high representing "totally disagree" to "completely agree." Specifically, the two variables of boundary coordination—information relevance and information transparency—were adapted from the classic survey scales of Li et al. [14] and Awad and Krishnan [71]. Government regulation and industry self-discipline were mainly referred from the relevant scales of Xu et al. [19,37]. In the measurement of user perceived privacy risk, we used the measure item in the study of Dinev and Hart [52] and Malhotra et al. [21]. Their scale is accurate, reliable, and widely confirmed in the field of privacy research. Xu et al. [17] and Chang et al. [16] made a comprehensive and detailed description of perceived privacy control, and the variables related to privacy control in the current paper were adopted from their research. Privacy concern and trust can be regarded as multi-dimensional structural variables and a single-dimensional study. The relevant concept scales of Dinev and Hart et al. [52], Xu et al. [17] and Wu et al. [69] were used for situational adaptation. To ensure the instructions' adequacy, we first conducted a predictive test on the questionnaire among 30 students who had experienced app privacy authorization.

We revised and improved some questions based on their feedback. The final items and sources of each construct are shown in Appendix A. The original measurement items were all in English, but our questionnaire was mainly distributed to Chinese app users. Thus, we invited two bilingual researchers to first translate the English items into Chinese and then back-translate the final survey results into English.

### *4.2. Sample and Data Collection Procedure*

All respondents were recruited through WeChat, the most popular social media platform in China. Specifically, we designed this questionnaire on a professional online survey website labeled www.wjx.cn (accessed on 30 July 2021). The questionnaire was randomly distributed by the three authors to their WeChat friends, and the respondents were encouraged to re-distribute it to their friends and so on. Before the investigation, a brief background on app privacy authorization was presented at the very beginning of the questionnaire. For the sake of screening out the sample group with a mobile app authorization experience, we set up a jump item at the start and designed the first question as follows: "Have you authorized or publicly disclosed your personal information through mobile apps?". If the answer was "no," the questionnaire was automatically directed to the end section. Additionally, to ensure that each respondent had a clear understanding of the core issues when completing the form, especially with regard to relevance and transparency, in the questionnaire we virtualized a situation in which a social media app requests user authorization and asked the qualified respondents to answer questionnaire items based on their privacy perception [72]. Furthermore, detailed concepts of government legislation and industry self-regulation were provided before starting the questionnaire in order to ensure that they can comprehend institutional privacy assurance very well. Additionally, to increase the response and effectiveness rate, we provided each participant with random monetary incentives. The bonus would be automatically sent to the WeChat accounts of the valid participants after the authors reviewed all the submitted questionnaires.

We received 620 questionnaires, of which 552 were complete. To ensure a high level of data quality, we removed an additional 63 questionnaires with identical scores for all indicator items, and filtered out 36 questionnaires with duplicate submissions from the same IP. Finally, we collected 453 valid responses, minimizing common method bias. Table 1 summarizes the sample demographics.

**Table 1.** Respondent personal information.

| Characteristics | Respondents (*n* = 453) | | |
|---|---|---|---|
| | **Items** | **Frequency** | **Percentage** |
| Gender | Male | 259 | 57.17 |
| | Female | 194 | 42.83 |
| Age (years) | <20 | 104 | 22.96 |
| | 20–35 | 217 | 47.90 |
| | 35–50 | 102 | 22.52 |
| | >50 | 30 | 6.62 |
| Platform | Android | 286 | 63.13 |
| | iPhone OS | 165 | 36.42 |
| | Others | 2 | 0.5 |
| Education | Less than high school | 65 | 14.35 |
| | College or university | 174 | 38.41 |
| | Advanced degree | 214 | 47.24 |
| Occupation | Student | 116 | 25.61 |
| | Official worker | 92 | 20.31 |
| | Researcher | 65 | 14.35 |
| | Enterprise staffs | 103 | 22.74 |
| | Self-employer | 43 | 9.49 |
| | Retiree | 27 | 5.96 |
| | Other | 7 | 1.54 |

## 5. Data Analysis

In this part, we first tested the common method variance (CMV), reliability and validity (convergent validity and discriminant validity) of the measurement model, and then the corresponding hypotheses and the appropriateness of the research model was verified through structural model analysis.

### 5.1. Common Method Variance

As a form of systematic error, common method variance (CMV) is commonly identified as a potential problem in homogenous data research. In this study, even though we conducted anonymous surveys on the respondents following the suggestion of Podsakoff et al. [73], the results may still suffer from CMV on account of the dependent variables and independent variables being extracted from a single survey. Thus, the confirmatory factor analysis was applied on the data. Results showed that the key fit indicators, such as $\chi^2$/df, the Root Mean Square Error of approximation (RMSEA), the Root Mean-square Residual (RMR), the Goodness of Fit Index (GFI) and the Comparative Fit Index (CFI) values, were all within the specified range, indicating that there was no significant CMV among the collected data. The results are demonstrated in Table 2.

**Table 2.** Fitting index of CMV.

| Fit Indices | $\chi^2/df$ | GFI | RMSEA | RMR | CFI | NFI | AGFI | PGFI | PNFI |
|---|---|---|---|---|---|---|---|---|---|
| Recommended value | <3 | >0.9 | <0.10 | <0.08 | >0.9 | >0.9 | >0.8 | >0.5 | >0.5 |
| Actual value | 1.745 | 0.937 | 0.038 | 0.071 | 0.985 | 0.965 | 0.908 | 0.985 | 0.638 |

### 5.2. Reliability and Validity

In the first step, confirmatory factor analysis (CFA) was performed by using SPSSAU. The scores of several key model fitting indexes are all in the reasonable range, including $\chi^2$/df = 1.478, GFI = 0.930, RMSEA = 0.033, RMR = 0.024, CFI = 0.987, NFI = 0.962, AGFI = 0.910, PGFI = 0.729 and PNFI = 0.808, which show a good fit of the hypothesized model to the data.

Furthermore, we performed the reliability, convergent validity and discriminant validity of all constructs. The reliability was validated by examining Cronbach Alpha value

(>0.7), composite reliability (CR) (>0.7) and average variance extracted (AVE) (>0.5) [74]. As shown in Table 3, all the Cronbach Alpha values, composite reliabilities and AVEs were larger than the relevant benchmarks, respectively. To summarize, the results embody the internal consistency and adequate reliability.

**Table 3.** Standardized item loadings, AVE, CR and Alpha values.

| Factor | Item | Standardized Item Loading | AVE | CR | Cronbach's $\alpha$ |
|---|---|---|---|---|---|
| Information Relevance | AR1 | 0.916 | 0.818 | 0.931 | 0.930 |
| | AR2 | 0.908 | | | |
| | AR3 | 0.888 | | | |
| Information Transparency | AA1 | 0.916 | 0.839 | 0.940 | 0.940 |
| | AA2 | 0.926 | | | |
| | AA3 | 0.907 | | | |
| Government Regulation | GR1 | 0.820 | 0.738 | 0.848 | 0.837 |
| | GR2 | 0.878 | | | |
| Industry Self-discipline | ISR1 | 0.865 | 0.853 | 0.921 | 0.920 |
| | ISR2 | 0.985 | | | |
| Perceived Privacy Control | PPC1 | 0.911 | 0.832 | 0.952 | 0.952 |
| | PPC2 | 0.907 | | | |
| | PPC3 | 0.913 | | | |
| | PPC4 | 0.918 | | | |
| Perceived Privacy Risk | PPR1 | 0.910 | 0.848 | 0.957 | 0.957 |
| | PPR2 | 0.913 | | | |
| | PPR3 | 0.929 | | | |
| | PPR4 | 0.931 | | | |
| Privacy Concern | PC1 | 0.916 | 0.829 | 0.951 | 0.951 |
| | PC2 | 0.919 | | | |
| | PC3 | 0.898 | | | |
| | PC4 | 0.911 | | | |
| Trust | TRU1 | 0.923 | 0.844 | 0.956 | 0.956 |
| | TRU2 | 0.913 | | | |
| | TRU3 | 0.911 | | | |
| | TRU4 | 0.929 | | | |
| Authorizing Intention | AI1 | 0.902 | 0.835 | 0.938 | 0.938 |
| | AI2 | 0.925 | | | |
| | AI3 | 0.916 | | | |

**Notes:** Composite reliability (CR) = (square of the summation of the factor loading)/[(square of the summation of the factor loadings) + (square of the summation of the error variance)]; average variance extracted (AVE) = (summation of the square of the factor loadings)/[(summation of the square of the factor loadings) + (summation of the error variances)].

It typically investigates the convergent validity, which evaluates whether each item could effectively reflect its corresponding factor with three metrics: the standardized factor loading is greater than 0.7 and reaches a significant level ($p < 0.05$ or $p < 0.01$), the composite reliability (CR) is above 0.7 and the average variance extracted (AVE) exceed the threshold of 0.5 [74]. Table 3 summarizes the statistical results. In addition to the CRs and AVEs exhibited above, all item loadings are ranged from 0.820 to 0.985. Thus, the scale proves a good convergent validity.

To test the discriminative validity of the constructs, we took two approaches of exploratory factor analysis (EFA) and confirmatory factor analysis (CFA). As for exploratory factor analysis (EFA), it is suggested that the loadings of each item on its respective construct should be higher than those on other constructs. Meanwhile, all the load coefficient values must exceed 0.7 [75]. Table 4 displayed the results of all constructs' loadings and cross-loadings, which represents a good discriminant validity.

**Table 4.** Construct cross-loadings.

| | Factor1 | Factor2 | Factor3 | Factor4 | Factor5 | Factor6 | Factor7 | Factor8 | Factor9 |
|---|---|---|---|---|---|---|---|---|---|
| IR1 | −0.114 | 0.014 | 0.063 | 0.001 | 0.014 | −0.018 | 0.935 | 0.009 | −0.024 |
| IR2 | −0.092 | 0.004 | 0.116 | −0.012 | 0.002 | 0.009 | 0.925 | −0.056 | 0.016 |
| IR3 | −0.095 | 0.006 | 0.082 | 0.012 | 0.015 | −0.010 | 0.923 | −0.027 | 0.002 |
| IT1 | −0.105 | −0.013 | 0.127 | −0.021 | 0.928 | 0.010 | 0.005 | 0.014 | −0.029 |
| IT2 | −0.094 | 0.016 | 0.123 | −0.006 | 0.933 | 0.037 | 0.024 | 0.012 | −0.007 |
| IT3 | −0.081 | −0.004 | 0.104 | 0.021 | 0.921 | 0.040 | 0.003 | 0.008 | −0.007 |
| GR1 | −0.078 | −0.028 | 0.085 | −0.017 | −0.033 | −0.079 | 0.048 | −0.001 | 0.922 |
| GR2 | −0.103 | 0.037 | 0.132 | −0.054 | −0.008 | −0.025 | −0.057 | −0.043 | 0.910 |
| ISD1 | 0.010 | 0.042 | 0.094 | 0.001 | 0.037 | 0.017 | −0.039 | 0.954 | −0.008 |
| ISD2 | 0.005 | 0.020 | 0.102 | 0.025 | −0.006 | −0.011 | −0.031 | 0.932 | −0.035 |
| PPC1 | −0.103 | −0.140 | 0.902 | 0.159 | 0.085 | 0.002 | 0.059 | 0.054 | 0.040 |
| PPC2 | −0.130 | −0.157 | 0.878 | 0.148 | 0.126 | 0.021 | 0.078 | 0.056 | 0.078 |
| PPC3 | −0.081 | −0.151 | 0.884 | 0.174 | 0.123 | 0.065 | 0.079 | 0.072 | 0.082 |
| PPC4 | −0.118 | −0.191 | 0.878 | 0.160 | 0.097 | 0.004 | 0.106 | 0.071 | 0.084 |
| PPR1 | 0.902 | 0.120 | −0.106 | −0.184 | −0.101 | −0.014 | −0.056 | 0.008 | −0.032 |
| PPR2 | 0.891 | 0.128 | −0.113 | −0.198 | −0.073 | −0.025 | −0.109 | 0.038 | −0.036 |
| PPR3 | 0.897 | 0.165 | −0.110 | −0.144 | −0.094 | −0.010 | −0.114 | 0.011 | −0.089 |
| PPR4 | 0.906 | 0.130 | −0.097 | −0.175 | −0.069 | −0.049 | −0.087 | −0.039 | −0.077 |
| PC1 | 0.147 | 0.897 | −0.137 | −0.165 | −0.016 | −0.093 | −0.004 | 0.047 | −0.004 |
| PC2 | 0.138 | 0.891 | −0.163 | −0.130 | 0.010 | −0.140 | 0.010 | 0.005 | −0.012 |
| PC3 | 0.120 | 0.873 | −0.174 | −0.149 | 0.008 | −0.177 | 0.016 | −0.004 | 0.014 |
| PC4 | 0.135 | 0.890 | −0.153 | −0.154 | −0.006 | −0.116 | 0.006 | 0.029 | 0.008 |
| TRU1 | −0.206 | −0.157 | 0.167 | 0.870 | −0.011 | 0.179 | −0.007 | −0.006 | −0.024 |
| TRU2 | −0.145 | −0.179 | 0.138 | 0.883 | −0.004 | 0.174 | 0.016 | 0.014 | −0.048 |
| TRU3 | −0.188 | −0.143 | 0.202 | 0.869 | −0.009 | 0.157 | −0.019 | 0.028 | −0.005 |
| TRU4 | −0.214 | −0.159 | 0.170 | 0.873 | 0.020 | 0.168 | 0.010 | −0.001 | −0.016 |
| AI1 | −0.064 | −0.154 | 0.034 | 0.248 | 0.023 | 0.885 | 0.016 | −0.013 | −0.034 |
| AI2 | −0.013 | −0.170 | 0.015 | 0.162 | 0.048 | 0.916 | −0.046 | 0.030 | −0.030 |
| AI3 | −0.007 | −0.146 | 0.025 | 0.169 | 0.023 | 0.910 | 0.010 | −0.009 | −0.056 |

Confirmatory factor analysis (CFA) is performed to ensure sufficient discriminant validity. Specifically, we did a test in respect of whether each construct's square root of the AVE greater than the correlation coefficient with other variables [76]. Our findings demonstrated in Table 5 indicated that each variable is more relevant to its own than to the rest of other variables, fulfilling the above requirement. Combining the analysis results of the above two methods, the discriminant validity was then satisfied.

**Table 5.** Correlation coefficients and square root of AVE.

| | IR | IT | GR | ISR | PPC | PPR | PC | TRU | AI |
|---|---|---|---|---|---|---|---|---|---|
| IR | 0.864 | | | | | | | | |
| IT | −0.035 | 0.921 | | | | | | | |
| GR | 0.014 | −0.053 | 0.906 | | | | | | |
| ISD | −0.014 | 0.04 | 0.043 | 0.915 | | | | | |
| PPC | 0.184 | 0.156 | 0.183 | 0.245 | 0.913 | | | | |
| PPR | −0.155 | 0.006 | −0.208 | −0.197 | −0.297 | 0.923 | | | |
| PC | −0.014 | 0.032 | −0.015 | −0.042 | −0.367 | 0.326 | 0.910 | | |
| TRU | −0.031 | 0.034 | 0.035 | 0.046 | 0.385 | −0.412 | −0.395 | 0.919 | |
| AI | −0.099 | 0.007 | −0.009 | 0.069 | 0.116 | −0.118 | −0.336 | 0.405 | 0.911 |

### *5.3. Data Analysis and Results*

With the statistical analysis tool of SMART PLS 2.0, the research model is empirically analyzed employing partial least square (PLS). We specified the standardized path coefficients to test the relationship of all constructs. To further assess the significance of the paths, t-statistics generated by the standard bootstrap re-sampling procedure (500 samples) was adopted. Additionally, the square of the determinable coefficient ($R^2$) of all the five dependent variables were 0.2235, 0.1938, 0.3036, 0.2996, 0.2437, consecutively, indicating the degree of fit of the regression line to the observed values. As can be observed from Table 6, the PLS-SEM analysis indicated that all but one hypothesis was supported.

**Table 6.** Summary of hypotheses testing results.

| Hypotheses | Path Coefficients | *t*-Value | *p* Value | Results |
|---|---|---|---|---|
| H1 (IR- > PPC) | 0.1669 | 3.7352 | 0.0001 | Supported |
| H2 (IR- > PPR) | −0.1803 | 4.1366 | 0.0000 | Supported |
| H3 (IT- > PPC) | 0.2235 | 5.0023 | 0.0000 | Supported |
| H4 (IT- > PPR) | −0.1293 | 2.7794 | 0.0043 | Supported |
| H5 (GR- > PPC) | 0.2001 | 4.7322 | 0.0000 | Supported |
| H6 (GR- > PPR) | −0.1033 | 2.3004 | 0.0185 | Supported |
| H7 (ISD- > PPC) | 0.1669 | 3.5630 | 0.0001 | Supported |
| H8 (ISD- > PPR) | 0.0398 | 0.6517 | 0.3670 | Unsupported |
| H9 (PPC- > PC) | −0.2336 | 6.0143 | 0.0000 | Supported |
| H10 (PPC- > TRU) | 0.2315 | 4.8653 | 0.0000 | Supported |
| H11 (PPC- > PPR) | −0.2001 | 4.3221 | 0.0000 | Supported |
| H12 (PPR- > PC) | 0.2417 | 5.3316 | 0.0000 | Supported |
| H13 (PPR- > TRU) | −0.2022 | 5.2771 | 0.0000 | Supported |
| H14 (PC- > AI) | −0.2214 | 4.4457 | 0.0000 | Supported |
| H15 (PC- > TRU) | −0.2375 | 5.1223 | 0.0000 | Supported |
| H16 (TRU- > AI) | 0.2805 | 6.1744 | 0.0000 | Supported |

Of the antecedents, only industry self-regulation ($\beta = 0.0398$, $p > 0.05$) was found to have no obvious effect on users' perceived privacy risk. Apart from that, information relevance ($\beta = -0.1803$, $p < 0.001$), information transparency ($\beta = -0.1293$, $p < 0.05$), government regulation ($\beta = -0.1033$, $p < 0.05$) were all negatively related to risk perception. Therefore, H2, H4 and H6 were confirmed. Meanwhile, individuals' perceived privacy control can be strengthened by information relevance ($\beta = 0.1669$, $p < 0.001$), information transparency ($\beta = 0.2235$, $p < 0.001$), government regulation ($\beta = 0.2001$, $p < 0.001$) and self-regulation ($\beta = 0.1669$, $p < 0.001$). As such, the results for H1, H3, H5 and H7 were supported. For risk-control assessment, perceived privacy control has negative significant effects on privacy concern ($\beta = -0.2336$, $p < 0.001$) but positive significant effects on trust ($\beta = 0.2315$, $p < 0.001$), while the positive correlation between perceived privacy risk and privacy concern ($\beta = 0.2417$, $p < 0.001$), the negative correlation between perceived privacy risk and trust ($\beta = -0.2022$, $p < 0.001$) have been exhibited. Therefore, H9, H10, H12 and H13 were supported. Furthermore, there was a negative relationship between the two variables of control and risk ($\beta = -0.2001$, $p < 0.001$), thus supporting H11. As expected, privacy concern ($\beta = -0.2214$, $p < 0.000$) and trust ($\beta = 0.2805$, $p < 0.003$) both significantly influence users' authorizing intention as hypothesized, thus supporting H14 and H16. H15 was tenable by reason of privacy concern having a negative impact on trust ($\beta = -0.2375$, $p < 0.003$).

## 6. Discussion and Implications

### *6.1. Discussion*

This study develops and tests a framework of app users' privacy authorization and its correlates. Based on CPM theory, we expound that app users' intention of information authorization is a cognitive process involving boundary coordination and boundary turbulence, boundary rule formation and boundary self-regulation. Overall, the empirical results support 15 of the 16 hypotheses. Predictably, both privacy boundary coordination constructs play a significant role in boundary formation. Specifically, information relevance and information transparency have a positive impact on the perceived privacy control and a negative impact on perceived privacy risk of app users. These indicate that app providers must consider whether the functions are compatible with their services when designing and displaying the permissions required by users. Furthermore, the corresponding information purposes and storage methods should be clarified in the privacy policy.

In addition, government regulation has a significant influence on users' perceptions of privacy control and privacy risk, thus supporting H5 and H6. This finding indicates that the improvement and enforcement of laws and regulations can dramatically advance users' sense of privacy control and relieve their risk awareness, consistent with domestic and international research. Although the idea that industry self-regulation enhances individuals' perceptions of privacy control lends support to H7, the finding of H8 does not live up to expectations. This unconfirmed result is in line with Xu et al. [17], who stated that industry self-regulation does not alleviate users' perception of privacy risk for any of the site contexts. Similarly, Hui et al. [77] also concluded that privacy seals may well be ineffective in mitigating privacy risks. One possibility is that the privacy protection services provided by the industry, such as the establishment of industry alliances, the introduction of alliance standard policies, or the provision of evaluations and certifications by third parties, are poorly understood by app users. Hence, the follow-up propaganda of the third-party organizations, such as industry associations, is essential.

During the initial formation of privacy boundaries to safeguard self-regulation, app users' privacy concern is fueled by their perceived privacy risk and their privacy being out of control. Correspondingly, perceptions of privacy control and privacy risks have opposite effects on shaping an individual's trust; hence, H9, H10, H12, and H13 are all confirmed. Meanwhile, perceived privacy control plays an obvious role in alleviating perceived privacy risks, thus supporting H11. These partially demonstrated findings in the studies of Wang et al. [78], Degirmenci [64] and Libaque-Sáenz [36] are confirmed yet again in the context of mobile app privacy authorization. In the last phase, it is profoundly implied that privacy concern and trust are the decisive forces influencing users' privacy boundary decisions and that user trust has a greater impact on their willingness to authorize their information than their privacy concern. Thus, establishing and retaining user trust and offering sufficient reassurance on the consequences of the user information disclosure are requisite steps for every app provider.

### 6.2. *Implications for Theory and Manager*

The findings of this study highlight several theoretical and practical implications. In terms of theoretical contributions, first, it builds a consolidated model to elaborate individual privacy boundary management processes. Existing literatures gave more weight to the fragmented perspectives of privacy rather than a comprehensive privacy mechanism. Hence, an integrated model that enables us to differentiate and make out the variance adequately in perceived privacy concepts is required. By extending the CPM theory to the mobile app domain, we further introduce the IPA theory and FIR principle into the privacy context, which more comprehensively demonstrates the privacy decision-making process of individuals, improves the explanatory power of CPM theory in the mobile app authorization context, and contributes conducive value to the further development of privacy literature.

Second, privacy management is not only a matter of individual behavior, but embodies an important aspect of the institutional structure of the government and the industry as a whole. Yet many studies inclined to account for perceived privacy just with the constructs of individual level. To supplement this, this paper shed light on the important role of government regulation and industry self-regulation in shaping users' privacy perception and in turn privacy intention, which paves the terrain for the study of how to combine the inherent demand of user privacy protection with national and industrial privacy protection policies, and then facilitates boundary decision-making of privacy at the individual level.

Third, it provides a rich and detailed understanding of information relevance and transparency in the context of mobile apps. Most previous research treated the FTP Principle as an entity to explore the impact of institutional guidelines on individual privacy assessment. In this paper, the relevance and transparency of authorized information, two elements we distill from the FTP principle, were used as antecedent variables to influence users' privacy decisions, which is also uncommon in privacy-related studies. It is manifested that both elements contribute to users' positive privacy perceptions when authorizing personal information, which also extends the dimensions of the study of the FTP Principle and enriches the determinants of users' risk control perceptions.

Last but not least, it reaffirms the previous findings that privacy concerns and trust beliefs are pivotal variables to account for app users' willingness to provide their personal information, and that users' risk-control perceptions are inextricably bound up with their formation of privacy concerns and trust. Furthermore, we bring a vital, valuable insight into the relationship between perceived privacy risk and perceived privacy risk control, as well as privacy concerns and trust, which fully illustrates that privacy decision making is a complex profit-and-loss calculation or game process, and further enriches the privacy calculus model.

This empirical study has implications for practitioners as well. First, in response to ever-growing privacy incidents and volatile economic surroundings, many international organizations and countries have implemented privacy legislation. For instance, the FIP Principle and other privacy regulations were first developed in the United States, and the General Data Protection Regulation (GDPR) adopted by the European Union is the most stringent data protection law in history, which sheds light on the fact that privacy supervision has reached an unprecedented level. Based on the user's perspective, it is concluded that strict government supervision of the collection and use of personal information by companies facilitates their belief in control and alleviates their risk awareness. To protect users' privacy rights and interests, and create a favorable environment for data interaction and propel the benign development of mobile app industry, effective measures should be taken, such as a sound legal system covering correlative laws, regulations, policies and standards, to bolster privacy protection in sync with taking full advantage of data resources for national development and industrial innovation.

Second, industry self-discipline is a significant force to standardize the privacy practice of enterprise and construct a good ordered market. However, the research results show that app users have no obvious perception of the effectiveness of industry self-discipline, which indicates that the current status of industry self-discipline in the field of app personal information protection needs to be improved urgently. Therefore, industry standards or norms related to personal information protection should be actively promulgated by industry associations and other third-party institutions. Additionally, testing and assessing the compliance of apps with respect to the collection and use of personal information while gaining publicity is also a worthwhile initiative to give full play to the important role of industry self-discipline in user information privacy protection.

Third, when users are conscious that their authorization information is tightly bound to core functions of the mobile apps and are as explicitly informed how their personal data would be collected and used, they will enjoy the feeling of privacy control and their perception of risk will be proportionately weakened. Accordingly, reducing unnecessary requests for permission and respecting users' right to make their own choices is the top priority for app providers. Likewise, it may be necessary to provide more clear instructions in app's privacy policies, such as clarifying the purpose of access and the information's application scope before requesting permission, which will enable users to manage their personal data with efficiency and ascertain whether their information is being handled properly. The above-mentioned measures will not only eliminate users' authorizing concern and better expand potential app users, but be more conducive to increasing the brand image of the apps, boosting the reputations of the enterprise, and benefitting the app providers in the long run.

## 7. Limitation and Future Direction

Privacy boundary management is a complex process, and in this paper we attempted to capture the process of privacy boundary coordination and formation by analyzing individuals' perceptions at a different level. However, limitations of the study are inevitable, and primarily focus on the following four aspects.

First, privacy decisions are known to be constrained by specific contexts, but privacy research should consider contextual differences. The study of user privacy decisions in this paper is limited to the context of app authorization, which more or less weakens the explanatory power of the findings at a broader level. In the future, we will continue our efforts to validate the model and findings in other privacy contexts.

In addition, the majority of the respondents in this paper are Chinese citizens, whose perceptions of external forces of privacy protection are based on the current privacy situation in China, including the power of government regulation, the degree of industry management, and the strength of privacy policy interpretation. However, the degree of policy improvement and enforcement of privacy protection varies from country to country. To examine the impact of these factors on privacy boundary formation more accurately, future research can collect data from users in other countries with different degrees of privacy protection implementation and enforcement.

What is more, the effective sample size for this analysis is 453, which exceeds the number of analyzed items by 10 times, and the sample size is moderate. In the follow-up study, we can further expand the sample size, which can reduce the common method bias and social desirability bias caused by the insufficiency of sample size [79]. In the future questionnaire design, apart from counting respondents' occupational categories, it will be essential to avoid the over-concentration of their work areas, which will also cause sample bias and affect the objectivity of the study findings.

Last but not least, here we only explore users' willingness to authorize their personal information by taking all the apps as a whole. However, users would actually have different privacy sensitivities and authorization judgments for various types of apps. To some extent, the findings may be considered more targeted and reliable if they rely on multiple scenarios to explore the user's privacy decisions for mobile apps. Following existing research, extension of the research background to different types of mobile apps and further supplementation the privacy studies in this thesis would be a good attempt.

**Author Contributions:** Conceptualization, J.T. and B.Z.; Data curation, J.T. and U.A.; Formal analysis, J.T. and B.Z.; Funding acquisition, B.Z. and U.A.; Methodology, J.T., B.Z. and U.A.; Project administration, B.Z. and U.A.; Resources, J.T.; Software, J.T.; Supervision, B.Z. and U.A.; Validation, J.T.; Visualization, J.T.; Writing – original draft, J.T.; Writing—review & editing, B.Z. and U.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

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

## Appendix A

**Table A1.** The final items and sources of each construct.

| Construct | Item | Wording |
|---|---|---|
| Information Relevance | IR1 | The information requested by this app is relevant to the service it provides. |
| | IR2 | The information requested by this app is related to an app's core function. |
| | IR3 | The information requested by this app looks appropriate for its functionality and service implementation. |

**Table A1.** *Cont.*

| Construct | Item | Wording |
|---|---|---|
| Information Transparency | IT1 | This app clearly states what types of personal information are collected from me. |
| | IT2 | This app details how my personal information is used. |
| | IT3 | This app clearly explains how to store and protect my personal information. |
| Government regulation | GR1 | I am aware of the laws or regulations that protect my authorized personal information. |
| | GR2 | These laws or regulations relating to the protection of personal information will protect my authorized information. |
| Industry self-discipline | ISD1 | I am aware of relevant industry self-discipline organizations, trade associations or third-party certification bodies that can protect my authorized information. |
| | ISD2 | These self-regulatory organizations, trade associations or third-party certification bodies related to the protection of personal information will protect my authorized information. |
| Perceived privacy control | PPC1 | I feel in control over who can get access to my personal information authorized by this app. |
| | PPC2 | I feel in control over what personal information is released by this app. |
| | PPC3 | I feel in control over how personal information is used by this app. |
| | PPC4 | In general, I think I can control the personal information that I have authorized to this app. |
| Perceived privacy risk | PPR1 | There is high potential for privacy loss associated with giving personal information to this app. |
| | PPR2 | I think that my authorized information could be inappropriately used by this app. |
| | PPR3 | Authorizing or providing my personal information to this app would involve unexpected problems. |
| | PPR4 | In general, it is risky to authorize personal information to this app. |
| Privacy Concern | PC1 | I am concerned that this app will over-collect my personal information |
| | PC2 | I am concerned that the personal information stored in this app could be misused |
| | PC3 | I am concerned that this app will leak my personal information to unauthorized third-party agencies |
| | PC4 | I am concerned that my personal information is at risk due to errors and omissions of data users |
| Trust | TR1 | This app is trustworthy in authorizing my personal information. |
| | TR2 | I trust that this app will tell the truth and fulfill promises related to my personal information. |
| | TR3 | I trust that this app will keep my best interests in mind when dealing with personal information. |
| | TR4 | I trust that this app is always honest with users when it comes to using the information that I would provide. |
| Authorizing Intention | AI1 | At the right time, I intend to authorize my personal information to the app background |
| | AI2 | In the future, I will probably authorize my personal information to the app background |
| | AI3 | In the future, I would like to authorize my personal information to the app background |

## References

1. Roesner, F.; Kohno, T.; Moshchuk, A.; Parno, B.; Wang, H.J.; Cowan, C. User-driven access control: Rethinking permission granting in modern operating systems. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 20–23 May 2012; pp. 224–238.
2. Erevelles, S.; Fukawa, N.; Swayne, L. Big Data consumer analytics and the transformation of marketing. *J. Bus. Res.* **2016**, *69*, 897–904. [CrossRef]
3. Harris, M.A.; Brookshire, R.; Chin, A.G. Identifying factors influencing consumers' intent to install mobile applications. *Int. J. Inf. Manag.* **2016**, *36*, 441–450. [CrossRef]
4. Shah, M.H.; Peikari, H.R.; Yasin, N.M. The determinants of individuals' perceived e-security: Evidence from Malaysia. *Int. J. Inf. Manag.* **2014**, *34*, 48–57. [CrossRef]
5. Shakhovska, N.; Fedushko, S.; Melnykova, N.; Shvorob, I.; Syerov, Y. Big Data analysis in development of personalized medical system. *Procedia Comput. Sci.* **2019**, *160*, 229–234. [CrossRef]
6. Choi, B.C.; Land, L. The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. *Inf. Manag.* **2016**, *53*, 868–877. [CrossRef]
7. Petronio, S. *Boundaries of Privacy*; State University of New York: Albany, NY, USA, 2002.
8. Pentina, I.; Zhang, L.; Bata, H.; Chen, Y. Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Comput. Hum. Behav.* **2016**, *65*, 409–419. [CrossRef]
9. Xu, R.; Frey, R.M.; Fleisch, E.; Ilic, A. Understanding the impact of personality traits on mobile app adoption–Insights from a large-scale field study. *Comput. Hum. Behav.* **2016**, *62*, 244–256. [CrossRef]
10. Li, P.; Cho, H.; Goh, Z.H. Unpacking the process of privacy management and self-disclosure from the perspectives of regulatory focus and privacy calculus. *Telemat. Inform.* **2019**, *41*, 114–125. [CrossRef]
11. Yeh, C.H.; Wang, Y.S.; Lin, S.J.; Tseng, T.H.; Lin, H.H.; Shih, Y.W.; Lai, Y.H. What drives internet users' willingness to provide personal information? *Online Inf. Rev.* **2018**, *42*, 923–939. [CrossRef]
12. Wottrich, V.M.; van Reijmersdal, E.A.; Smit, E.G. The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decis. Support Syst.* **2018**, *106*, 44–52. [CrossRef]
13. Baruh, L.; Secinti, E.; Cemalcilar, Z. Online privacy concerns and privacy management: A meta-analytical review. *J. Commun.* **2017**, *67*, 26–53. [CrossRef]
14. Sutanto, J.; Palme, E.; Tan, C.H.; Phang, C.W. Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Q.* **2013**, *37*, 1141–1164. [CrossRef]
15. Child, J.T.; Haridakis, P.M.; Petronio, S. Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Comput. Hum. Behav.* **2012**, *28*, 1859–1872. [CrossRef]
16. 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]
17. Xu, H.; Dinev, T.; Smith, J.; Hart, P. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *J. Assoc. Inf. Syst.* **2011**, *12*, 1. [CrossRef]
18. Widjaja, A.E.; Chen, J.V.; Sukoco, B.M.; Ha, Q.A. Understanding Users' Willingness to Put Their Personal Information on the Personal Cloud-Based Storage applications: An Empirical Study. *Comput. Hum. Behav.* **2019**, *91*, 167–185. [CrossRef]
19. Xu, H.; Teo, H.H.; Tan, B.C.; Agarwal, R. Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Inf. Syst. Res.* **2012**, *23*, 1342–1363. [CrossRef]
20. Culnan, M.J.; Bies, R.J. Consumer privacy: Balancing economic and justice considerations. *J. Soc. Issues* **2003**, *59*, 323–342. [CrossRef]
21. 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]
22. Li, H.; Sarathy, R.; Xu, H. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decis. Support Syst.* **2011**, *51*, 434–445. [CrossRef]
23. Culnan, M.J.; Armstrong, P.K. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organ. Sci.* **1999**, *10*, 104–115. [CrossRef]
24. Solove, D.J. Taxonomy of privacy. *Univ. Pa. Law Rev.* **2006**, *335*, 335–409. [CrossRef]
25. Tang, Z.; Hu, Y.J.; Smith, M.D. Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *J. Manag. Inf. Syst.* **2008**, *24*, 153–173. [CrossRef]
26. 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]
27. King, N.J.; Raja, V.T. Protecting the privacy and security of sensitive customer data in the cloud. *Comput. Law Secur. Rev.* **2012**, *28*, 308–319. [CrossRef]
28. Metzger, M.J. Communication privacy management in electronic commerce. *J. Comput. Mediat. Commun.* **2007**, *12*, 335–361. [CrossRef]
29. Celsi, R.L.; Olson, J.C. The role of involvement in attention and comprehension processes. *J. Consum. Res.* **1988**, *15*, 210–224. [CrossRef]

30. Xu, Y.; Chen, Z. Relevance judgment: What do information users consider beyond topicality? *J. Am. Soc. Inf. Sci. Technol.* **2006**, *57*, 961–973. [CrossRef]
31. Stanton, J.M.; Stam, K. Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives. *Surveill. Soc.* **2003**, *1*, 152–190. [CrossRef]
32. Zimmer, J.C.; Arsal, R.; Al-Marzouq, M.; Moore, D.; Grover, V. Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure. *Decis. Support Syst.* **2010**, *48*, 395–406. [CrossRef]
33. Lyon, D.; Waldo, J.; Lin, H.S.; Millett, L.I. A Short History of Surveillance and Privacy in the United States. In *Engaging Privacy and Information Technology in a Digital Age*; National Academies Press: Washington, DC, USA, 2007.
34. Milne, G.R.; Culnan, M.J. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *J. Interact. Mark.* **2004**, *18*, 15–29. [CrossRef]
35. Zhou, L.; Wang, W.; Xu, J.D.; Liu, T.; Gu, J. Perceived information transparency in B2C e-commerce: An empirical investigation. *Inf. Manag.* **2018**, *55*, 912–927. [CrossRef]
36. 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]
37. Xu, H.; Teo, H.H.; Tan, B.C.; Agarwal, R. The role of push-pull technology in privacy calculus: The case of location-based services. *J. Manag. Inf. Syst.* **2009**, *26*, 135–174. [CrossRef]
38. Gibson, J.L.; Caldeira, G.A. The legal cultures of Europe. *Law Soc. Rev.* **1996**, *30*, 55–85. [CrossRef]
39. Zucker, L.G. Production of trust: Institutional sources of economic structure, 1840–1920. In *Research in Organizational Behavior*; Staw, B.M., Cummings, L.L., Eds.; JAI Press: Greenwich, CT, USA, 1986; Volume 8, pp. 53–111.
40. Spiro, W.G.; Houghteling, L.J. *The Dynamics of Law*, 2nd ed.; Harcourt Brace Jovanovich: New York, NY, USA, 1981.
41. CTIA. Best Practices and Guidelines for Location Based Services. The Cellular Telecommunications and Internet Association (CTIA). 2008. Available online: http://www.ctia.org/content/index.cfm/AID/11300 (accessed on 30 July 2021).
42. Kim, D.; Ferrin, D.; Rao, R. A trust-based consumer decision-making model in electronic commerce. *Decis. Support Syst.* **2008**, *44*, 544–564. [CrossRef]
43. Petronio, S. *Boundaries of Privacy: Dialectics of Disclosure*; Suny Press: Albany, NY, USA, 2012.
44. Petronio, S. Brief status report on communication privacy management theory. *J. Fam. Commun.* **2013**, *13*, 6–14. [CrossRef]
45. Xu, H.; Teo, H.H. Alleviating consumers' privacy concerns in location-based services: A psychological control perspective. In Proceedings of the International Conference on Information Systems, ICIS 2004, Washington, DC, USA, 12–15 December 2004.
46. Hajli, N.; Lin, X. Exploring the security of information sharing on social networking sites: The role of perceived control of information. *J. Bus. Ethics* **2016**, *133*, 111–123. [CrossRef]
47. Taddei, S.; Contena, B. Privacy, trust and control: Which relationships with online self-disclosure? *Comput. Hum. Behav.* **2013**, *29*, 821–826. [CrossRef]
48. Krasnova, H.; Spiekermann, S.; Koroleva, K.; Hildebrand, T. Online social networks: Why we disclose. *J. Inf. Technol.* **2010**, *25*, 109–125. [CrossRef]
49. Havlena, W.J.; DeSarbo, W.S. On the measurement of perceived consumer risk. *Decis. Sci.* **1991**, *22*, 927–939. [CrossRef]
50. Shaw, N.; Sergueeva, K. The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *Int. J. Inf. Manag.* **2019**, *45*, 44–55. [CrossRef]
51. Dowling, G.R.; Staelin, R. A model of perceived risk and intended risk-handling activity. *J. Consum. Res.* **1994**, *21*, 119–134. [CrossRef]
52. Dinev, T.; Hart, P. An extended privacy calculus model for e-commerce transactions. *Inf. Syst. Res.* **2006**, *17*, 61–80. [CrossRef]
53. Liu, C.; Marchewka, J.T.; Lu, J.; Yu, C.S. Beyond concern—A privacy-trust-behavioral intention model of electronic commerce. *Inf. Manag.* **2005**, *42*, 289–304. [CrossRef]
54. Kim, G.; Koo, H. The causal relationship between risk and trust in the online marketplace: A bidirectional perspective. *Comput. Hum. Behav.* **2016**, *55*, 1020–1029. [CrossRef]
55. Flavián, C.; Guinalíu, M.; Gurrea, R. The role played by perceived usability, satisfaction and consumer trust on website loyalty. *Inf. Manag.* **2006**, *43*, 1–14. [CrossRef]
56. 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]
57. Gashami, J.P.G.; Chang, Y.; Rho, J.J.; Park, M.C. Privacy concerns and benefits in SaaS adoption by individual users: A trade-off approach. *Inf. Dev.* **2016**, *32*, 837–852. [CrossRef]
58. Anderson, C.L.; Agarwal, R. The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Inf. Syst. Res.* **2011**, *22*, 469–490. [CrossRef]
59. Jung, Y.; Park, J. An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services. *Int. J. Inf. Manag.* **2018**, *43*, 15–24. [CrossRef]
60. Pavlou, P.A.; Liang, H.; Xue, Y. Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Q.* **2007**, *31*, 105–136. [CrossRef]
61. Balapour, A.; Nikkhah, H.R.; Sabherwal, R. Mobile application security: Role of perceived privacy as the predictor of security perceptions. *Int. J. Inf. Manag.* **2020**, *52*, 102063. [CrossRef]

62. Junglas, I.A.; Johnson, N.A.; Spitzmüller, C. Personality traits and concern for privacy: An empirical study in the context of location-based services. *Eur. J. Inf. Syst.* **2008**, *17*, 387–402. [CrossRef]
63. Bansal, G.; Zahedi, F.M.; Gefen, D. Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Inf. Manag.* **2016**, *53*, 1–21. [CrossRef]
64. Degirmenci, K. Mobile users' information privacy concerns and the role of app permission requests. *Int. J. Inf. Manag.* **2020**, *50*, 261–272. [CrossRef]
65. Van Dyke, T.P.; Midha, V.; Nemati, H. The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. *Electron. Mark.* **2007**, *17*, 68–81. [CrossRef]
66. Baptista, G.; Oliveira, T. Understanding mobile banking: The unified theory of acceptance and use of technology combined with cultural moderators. *Comput. Hum. Behav.* **2015**, *50*, 418–430. [CrossRef]
67. Van Slyke, C.; Shim, J.T.; Johnson, R.; Jiang, J.J. Concern for information privacy and online consumer purchasing. *J. Assoc. Inf. Syst.* **2006**, *7*, 16.
68. Schoenbachler, D.D.; Gordon, G.L. Trust and customer willingness to provide information in database-driven relationship marketing. *J. Interact. Mark.* **2002**, *16*, 2–16. [CrossRef]
69. 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]
70. Rosenthal, R.; Rosnow, R.L. Applying Hamlet's question to the ethical conduct of research: A conceptual addendum. *Am. Psychol.* **1984**, *39*, 561. [CrossRef]
71. Awad, N.F.; Krishnan, M.S. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Q.* **2006**, *30*, 13–28. [CrossRef]
72. Fang, Y.; Qureshi, I.; Sun, H.; McCole, P.; Ramsey, E.; Lim, K.H. Trust, satisfaction, and online repurchase intention. *MIS Q.* **2014**, *38*, 407–428. [CrossRef]
73. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.Y.; Podsakoff, N.P. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *J. Appl. Psychol.* **2003**, *88*, 879. [CrossRef]
74. Fornell, C.; Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
75. Nunnally, J.C. *Psychometric Theory*; McGraw-Hill Book Company: New York, NY, USA, 1978; pp. 86–113.
76. Barclay, D.; Thompson, R.; Higgins, C. The Partial Least Squares (PLS) approach to Causal Modeling: Personal Computer Adoption and Use an Illustration. *Technol. Stud.* **1995**, *2*, 285–309.
77. Hui, K.L.; Teo, H.H.; Lee, S.Y.T. The value of privacy assurance: An exploratory field experiment. *MIS Q.* **2007**, *31*, 19–33. [CrossRef]
78. Wang, T.; Duong, T.D.; Chen, C.C. Intention to disclose personal information via mobile applications: A privacy calculus perspective. *Int. J. Inf. Manag.* **2016**, *36*, 531–542. [CrossRef]
79. Gong, X.; Zhang, K.Z.; Chen, C.; Cheung, C.M.; Lee, M.K. What drives self-disclosure in mobile payment ap-plications? The effect of privacy assurance approaches, network externality, and technology complementarity. *Inf. Technol. People* **2019**, *33*, 1174–1213. [CrossRef]