Proactive privacy practices in transition: Toward ubiquitous services

Shu-Ching Wang, a, Jen-Her Wu b,∗

a Department of Information Management, National Kaohsiung Marine University, 142, Haijhuau Road, Nanzih District, Kaohsiung 81157, Taiwan, ROC
b Department of Information Management, National Sun Yat-Sen University, 70, Lien-Hai Road, Kaohsiung 80424, Taiwan, ROC

A R T I C L E   I N F O

Article history:
Received 10 August 2012
Received in revised form 27 August 2013
Accepted 26 September 2013
Available online 5 October 2013

Keywords:
Electronic services
Mobile services
Ubiquitous services
Mobile commerce
Ubiquitous Commerce
Proactive privacy governance
Disclosure willingness
Integrative social contracts theory

A B S T R A C T

As the Internet paved the way for electronic businesses, ubiquitous services (u-services) will be the next wave launched by electronic services based on current customer information potential. However, privacy is a strategic issue and has been identified as a key hindrance to u-services. As a proactive approach and drawing upon integrative social contracts theory, this study presents a proactive privacy practices framework to examine how the interplays within electronic service, providers’ proactive approaches influence customer disclosure willingness for future u-services, adoption. The results and implications of this study are discussed and expected to shed light on privacy practices.

© 2013 Published by Elsevier B.V.

1. Introduction

Ubiquitous services (u-services)—or ubiquitous commerce (u-commerce)—are a logical extension of today’s electronic services (e-services). They are likely to be the next wave in a new e-era (i.e., after e-services/e-commerce and mobile services/commerce) [26,37]. U-services can be introduced cost effectively by using existing customer pools for e-services and propagated by using new m-services. U-services have created new opportunities for businesses and have provided ways for businesses to interact with their customers, to collect relevant information and to achieve closer customer relationships by removing spatial and temporal restrictions. U-services can also be widely applied in diverse domains, such as health care, retail, transportation and banking.

More customized and personalized services can be provided in such context-aware networks. However, customers may be uncomfortable with the use of u-services because of privacy concerns related to u-services. The threat of the accidental or deliberate dissemination and use/reuse of personal information for unauthorized purposes is a critical impediment to u-service development and adoption [36]. Privacy concerns discourage people from submitting personal information and shopping online and are thus an obstacle preventing people from enjoying the convenience, diversity, and flexibility of e-services [42].

While some people value their privacy, others are willing to trade their personal information for benefits such as discounts or rewards. Effective solutions for privacy concerns are important for enterprises, governments and the public. Privacy is a strategic issue that deserves great attention from both scholars and practitioners because customer information is used in a variety of business processes and can be used in response to competitive pressures. Furthermore, gaining new customers is more expensive than retaining valuable ones [30]. Thus, information management has become an increasingly important issue due to the organizational and customer behavioral patterns involved [27,48,50,51].

Although most e-service providers (ESPs) provide their privacy practices online in response to consumer concerns, they can also take action to proactively interact with customers. This proactive interaction aims to alleviate consumer’s privacy concerns and to prevent privacy invasion. While numerous prior studies [1,8,19,24,25,29,48] have focused on trust, risk and privacy concerns and their impact on related online activities, such as transactions and disclosure behaviors, this study explores which privacy practices ESPs can use to interact with customers. Customer interaction allows ESPs to obtain real and useful customer information (e.g., mobile phone numbers) in order to
transition from providing e-services to providing u-services. In the u-service context, mobile communication devices are likely the most popular and effective way of reaching targeted customers at the right time and place. By contrast, mobile communication is not necessary in the typical e-service context. This study focuses on the transition of ESPs from e-services to u-services. A key question of interest to merchants and managers is as follows: what are the implications of using proactive privacy practices for customers? To answer this question, this study addresses the following set of questions: (1) What are the different ways an ESP can initiate privacy practice interactions with customers? (2) How do proactive privacy governance and u-service-related strategies affect customers’ disclosure willingness? (3) What are the associated interactions between proactive privacy governance and u-service-related strategies (i.e., perceived u-service value and value-added strategies) in relation to customers’ disclosure willingness?

Answers to such questions can help ESPs identify the strengths and weaknesses of their current privacy practices and thus allow them to develop more effective privacy practices to expand their current businesses toward u-services or u-businesses. Our study draws on integrative social contracts theory to develop a proactive privacy practice model and to explore its value in practice.

2. Conceptual development and research hypotheses

2.1. E-services vs. u-services

Many concepts related to e-services have been proposed. For example, e-services have been proposed for essential business functions, such as online catalogs and order fulfillment, as well as customer-centered and support activities. While Zhang et al. [49] has regarded e-services as an amalgamation of business processes, policies, procedures, tools, technology and human resources, in an attempt to enhance customer services, Featherman and Pavlou [18] regarded e-services as an interactive information system with special assets (such as information, business processes, computing resources, applications) that allows for the development of new revenue and increased efficiency.

It is believed that e-services are typically B2C and utilize e- and m-service processes that offer electronic communication, information collection, transaction processing, and data exchange in order to deliver core products and services in response to customers’ needs [17,43]. The e-service context has flaws, however, lacking automatic location detection, unique identity verification and context awareness of the physical environment. With the rapid growth and proliferation of e-services, e-services now are considered to be the driving force for u-services, facilitating the utilization of existing customer pools based on accessible, reliable and relevant customer information.

A constant aim for businesses is to establish more intimate relationships with their customers [4,51]. U-services have become one of the most efficient ways to establish intimate relationships with customers and convey innovation to customers, and they provide new opportunities to market businesses [27,37]. U-services utilize both the context awareness and intelligent applications embedded within mobile communication devices and are thus able to detect a customer’s unique identity and store and gather abundant information from and sense changes in the customer’s physical surroundings, including the people, objects, and events within and conditions of that environment. Customers are always connected seamlessly in these context-aware networks, allowing personalized services to be delivered in a timely manner [27]. The aim of u-services is to compensate for the shortcomings of e-services, to exponentially improve customer relationships and to support customer-related activities. Although u-services are more convenient and efficient, customers are becoming increasingly aware of the privacy threats related to u-services, which evolve and become more salient over time. These privacy threats and the potential for privacy invasion discourage customers from adopting and enjoying u-services.

2.2. Privacy issues

Customer privacy concerns are multi-dimensional, including improper acquisition of personal information (e.g., unauthorized access and collection of personal information; improper monitoring of online behavior), improper use of personal information (e.g., unauthorized sharing of personal information with third-party or affiliated companies), and privacy invasion (e.g., dissemination of personal information without a customer’s prior consent) [1,42]. Even reputable websites share customer information with their affiliated companies [29]. Although ESPs disclose their information practices by posting privacy policies and privacy seals, numerous studies have shown that such privacy policies are too complicated and thus are rarely read by customers [2,28,42].

Many customers are willing to trade their personal information for benefits such as rewards and discounts. People can generally be classified into three groups regarding their level of concern with privacy: privacy fundamentalists, privacy pragmatists and unconcerned customers. Most customers are privacy pragmatists, who assess the potential benefits and privacy risks of providing their information before deciding whether to disclose it [1,28].

While u-services seek to reach consumers anywhere and at any time and to provide customized and personalized services and products, u-service providers still face the challenge of obtaining personal information from customers who are privacy fundamentalists [1]. Privacy practices are thus crucial for ESP in coaxing customers to disclose their personal information [23,41,42].

2.3. Integrative social contracts theory

Integrative social contracts theory (ISCT) is based on social contract theory (SCT), which is generally applied to exchange relationships in the marketing and business domain. It has provided moral guidelines for businesses that are founded on impartiality and consent. For instance, Li et al. [29] examined information exchange as a fair social contract, whereas Spaulding [38] used SCT to determine how virtual communities create value for businesses. Generally, three core elements are included in such theories: (1) individual consent, (2) agreement among moral agents, and (3) a device or method whereby an agreement is obtained.

ISCT is more suited for ethical issues across different communities because it covers boundary-spanning relationships and cross-cultural problems. Within ISCT, “integrative” refers to the use of two different types of social contracts: a hypothetical macro-social contract that is employed as a heuristic approach and an actual micro-social contract that exists in relevant communities. Thus, ISCT is rooted in the social norms that are the underlying behavioral rules for living in a community. These communities may be as large as a nation state or corporation or as small as a department or informal unit [15,16].

Furthermore, certain behaviors are assumed to take place in forming contracts. In particular, rational reactions are assumed to occur between contractors, who face bounded moral rationality, as an extension of the economic rationality in the moral sphere. Information, time, and emotional strength may be insufficient to allow people to make perfect moral judgments, and global contractors may not be able to reach a perfect consensus. ISCT postulates that people work to preserve their right to choose their own values to the extent possible. In addition, people aspire to
become a part of economic communities in response to their individual and cultural values. The assumption is that global contractors are aware of the need for a community-based morality. Thus, global contractors should reach a consensus on the creation of a binding macro-social contract and provide arguments to support its effectiveness [15,16]. As such, all rational individuals are assumed to agree to its terms. The first two items of the macro-social contract according to ISCT are as follows:

1. Local economic communities may specify ethical norms for their members through micro-social contracts.
2. Norm-generating micro-social contracts must be grounded in informed consent, butressed by rights to exit the contract and to have voice (i.e., the "protected informed consent" term).

2.4. ISCT and proactive privacy governance

In line with the assumptions of ISCT, e-service customers confront their own limited capacity in comprehending and absorbing all the details related to e-service privacy. Often, e-service customers have insufficient information, which hinders their ability to make educated privacy-related decisions, or they are unfamiliar with a site's privacy practices [28,40,42]. Drawing upon ISCT, ESPs should implement proactive privacy practices, allowing for a type of procedural justice, which can be regarded as the community-based moral fabric in the B2C e-service context. Following the perspective of ISCT, online privacy practices should be constructed to require ESPs to handle customers' information in a responsible manner.

If privacy is important to customers in the online environment, an ESP who is privacy-friendly with more salient characteristics would gain a competitive advantage over its competitors [42]. Customers need to be aware of an ESP's privacy practices so that they can make meaningful decisions about whether to disclose their personal information online [2,40]. ESPs should protect consumers' privacy and use customers' personal information only with their informed consent. ESPs also need to identify ways to proactively and efficiently convey relevant privacy protection information to their customers. In this study, the use of proactive privacy practices is called "proactive privacy governance (PPG)". PPG relates to the actions that ESPs take to proactively protect customers' privacy not only in the e-service context but also in the u-service context.

Governance implies that activities that carry the same goals as purposive behavior, oriented activities and economic rule systems. It may or may not be a direct derivative from legal and formally prescribed responsibilities and does not need to rely on police powers to overcome defiance and attain compliance. Governance is the extent of enforcement of prescribed laws, rules and regulations [5]. Consequently, PPG is defined for this study as the initiative by an ESP to interact with customers to set the laws, rules, regulations, and values that govern customer privacy protection in an economic community [13]. The PPG measures that are used in this study aim to capture different facets of the interactions between customers and ESPs in the B2C e-service context.

From the consumer behavior perspective, rational consumers often obtain relevant information before making decisions online as a way to reduce their privacy concerns. Proactive privacy governance should therefore be able to fill or close the information gaps in customers' knowledge and make up for the finite human capacity to assess facts by proactively providing a comprehensive conception of the ESP's privacy practices to their customers. Derived from ISCT and acknowledging the importance of procedural justice of online decision making, PPG should embrace three practices: proactive provision and protection, proactive education, and proactive monitoring and feedback seeking. These practices are outlined below.

Proactive provision and protection (PPP) is defined as an ESP's proactive efforts to inform customers of their privacy practices and their respect for customers' rights and values through the use of specific, understandable expressions that improve customers' comprehension of their privacy practices. In the e-service context, with an understanding of an ESP's privacy practices, customers will feel more at ease and be better able to determine whether to disclose their personal information or to opt into u-services. PPP incorporates ideas from the primary two terms of the macro-social contract in ISCT and employs the principles of fair information practices (FIP) as a guide for professional conduct related policies. This is the rationale behind the practice of proactive provision and protection proposed in this study.

Proactive education (PE) refers to an ESP's proactive efforts to educate customers about their responsibilities in preventing privacy invasions and about the redress if a privacy invasion occurs. PE incorporates ideas from the bounded moral rationality assumption in ISCT that educate customers about their own responsibilities and obligations, about their security and privacy practices, and about the redress for privacy invasion. For instance, customers should have rights and must be instructed on how to enable disable their mobile device to opt in/opt out of u-services at their own convenience. PE is most important for those who lack knowledge about information technology and privacy protection. This is the rationale behind the practice of proactive education proposed in the study.

Proactive monitoring and feedback seeking (PMFS) is defined as an ESP's proactive efforts to monitor its privacy and security management practices, send alert messages if customers' information is compromised, and solicit or respond to their feedback in order to ensure that their rights and preferences are protected. PMFS incorporates ideas from the assumptions in ISCT that individual contractors join economic communities based on their personal values. Numerous ESPs now provide their privacy policies online but do not guarantee that they will comply with their privacy policies [2]. ESPs should demonstrate that they are capable of monitoring their privacy systems and protecting customers' rights. In a u-service context, PMFS should be used for services such as mobile payments, pay-by-phone services, and context-aware tour guides. Proactive monitoring and feedback seeking enables an ESP to send an alert message to customers if irregularities arise and to receive information from customers regarding their e-services usage experience. Such practices give customers and the ESP a "voice". Customers are likely to feel better if such a monitoring and feedback system allows them to have a strong voice [6]. It is essential that ESPs take action to monitor their privacy systems to prevent privacy invasions and to proactively collect feedback in order to respond to customers in a timely fashion. This is the rationale behind the practice of proactive monitoring and feedback seeking proposed by the authors.

The practices mentioned above are based on the consumer perspective and ISCT. It may be that consumers ignore important information within privacy policies due to time constraints or difficulties in recognizing their importance. The three proactive governance practices stated above would provide means to mitigate the possible concerns and risks resulting from information asymmetry. Prior studies [28,42] have recognized that online customers value information regarding how their personal information is used and how they can control its use. Whether an ESP provides its privacy practices online affects customers trust in the ESP, how customers perceive privacy policies and customers' willingness to disclose their information. The pragmatic conclusion
at this point is for ESPs to initiate communication with customers about their privacy governance, which is likely to alleviate customers' privacy concerns and encourage data disclosure. According to Awad and Krishnan [3], disclosure willingness refers to consumers' willingness to provide personal information that is needed for u-services, such as shopping and personalized services. According to ISCT, the use of proactive privacy governance will provide a more comprehensive picture of ESPs' privacy practices and positively affect information sharing. Hence, the following hypothesis is proposed:

H1. ESPs' use of proactive privacy governance will positively influence their customers' willingness to disclose the personal information needed for u-services.

2.5. ISCT and perceived value

According to ISCT, individuals aim to maintain the right to choose their own values and to participate in economic communities that reflect their personal and cultural values [15,16]. In our study, both e-services and u-services can be regarded as economic communities. Service providers should proactively conveying their privacy practices to customers and ensure that their customers understand these practices. From an economic perspective, an individual's perceived value of goods or services is essential in any economy, especially when he or she is contemplating whether to participate in a community.

The personal/cultural values or perceived value are in relation to individual differences and preferences that pertain to marketing strategies. Thus, according to Antón et al. [2], privacy practices should take into account human, economic, legal and technical perspectives. When ESPs endeavor to extend e-services to u-services, two essentials derived from the economic community perspective in ISCT need to be considered: (1) PPG provides a community-based moral fabric to maintain procedural justice and privacy assurance, and (2) the customers must be informed of the intrinsic value of u-services to enhance the perceived value of u-services and thus promote u-service adoption, especially at this early stage. The higher the perceived value that customers ascribe to u-services, the more willing they will be to disclose their information.

Generally speaking, customer perceived value refers to the benefits perceived from the customer's perspective; namely, the customer's subjective evaluation of the features and performance of a product/service and the results of the use of that product/service [47]. Perceived value can, usually, be conceptualized as a multidimensional construct that includes emotional, social, quality/performance and price/value components. Perceived value has also been acknowledged as an antecedent of satisfaction and behavioral intentions [39,44]. In our study, the notion of perceived u-service value is inspired by ISCT, but the operationalization of perceived u-service value is adapted from a prior study [39]. In this study, perceived u-service value is defined as “the consumer’s overall assessment of the utility and benefits of u-services based on perceptions of what is received and what is given”. Three dimensions (i.e., emotional, social, and functional) are examined for perceived u-service value. The definition for each dimension in this study is derived from Sweeney and Soutar [39]. While the emotional value is defined as the utility elicited from the feelings or affective states that u-services generate, the social value refers to the utility derived from the ability of u-services to improve social self-concept. Meanwhile, the functional value is regarded as the utility derived from the perceived quality and expected performance of a u-service. Consequently, based on ISCT and the multidimensional conceptualization of “perceived value”, the following hypothesis is proposed.

H2. A customer's perceived u-service value will positively influence his/her willingness to disclose the personal information needed for u-services.

2.6. ISCT, value-added strategies and moderating effects

In line with the assertions of ISCT, customers wish to take part in economic communities that are compatible with their own values and beliefs. In addition to the value of privacy assurance and the perceived values of u-services, ESPs should also use strategies (i.e., activities) to attract customers and increase customers' disclosure willingness. We call these activities value-added strategies, which is similar to the competitive strategy perspective [34] that emphasizes difference and deliberate selections of a diverse set of activities to convey a unique mix of value. Businesses must either demonstrate superior value to customers or deliver comparable value at a better price, or both, to stimulate customer behavior such as consuming, participating etc. Prior studies on consumer behavior have highlighted some crucial factors that affect individuals' intentional behavior: merchant reputation [6,25,28], personalized services [3,11,28,31], alliance-based services [7], and incentives, such as gifts, rewards or discounts [20,23,42]. Hence, the value-added strategies in our study are defined as a varied set of strategies, such as those taking into account the abovementioned factors, employed to convey a unique mix of value to customers [34].

Furthermore, according to Porter [33,34], an organization's competitive advantage results from the way that its activities fit and reinforce one another. Based on ISCT and the economic perspective, for an ESP striving to enter the u-service market at this early stage, its value-added strategies for u-services may be an important factor in persuading customers to disclose their personal information. Apart from adopting proactive privacy governance in the e-service context and informing customers of the inherent value of their u-services (i.e., perceived value), the value-added strategies should fit with and strengthen an ESP's PPG and perceived u-service value to promote its competitive advantage. This is also consistent with Venkatraman's [45] fit as moderation perspective. Fit is thus conceptualized as the interactions among an ESP’s PPG, perceived u-service value and value-added strategies.

This conceptualization of fit is logical when fit is theoretically anchored to a certain criterion variable, namely, customers’ disclosure willingness for u-services. The perspective has affirmative theoretical specificity, and the interactions between the predictors and moderator are the primary determinants of the criterion variable. Consequently, fit is examined regarding the interaction effect of the predictors and moderator on the criterion variable and can be theoretically linked to the complementarities concept as a positive interaction effect, in which an increase in one variable leads to an increase another variable [41]. In other words, value-added strategies should reinforce the effects of PPG and perceived u-service value on customers’ disclosure willingness. Thus, our study examines not only the main effect of value-added strategies on customers’ disclosure willingness but also the interactions among PPG, perceived value, and disclosure willingness. This leads to the following hypotheses.

H3a. ESPs’ value-added strategies will positively influence customers’ willingness to disclose the personal information needed for u-services.

H3b. ESPs’ value-added strategies will positively moderate the relationship between PPG and customers’ willingness to disclose the personal information needed for u-services.
H3c. ESPs’ value-added strategies will positively moderate the relationship between customers’ perceived u-service value and their willingness to disclose the personal information needed for u-services.

Based on ISCT, this study presents a comprehensive framework, the proactive privacy practice model (PPPM), that provides guidelines for ESPs in implementing better privacy practices to transition from providing e-services to providing u-services. The conceptual framework identifies the relevant technical, legal, human and economic perspectives that are required to support proactive privacy practices. The relationships among the important constructs are depicted in Fig. 1.

3. Research methodology

3.1. Research approach

This study consisted of two approaches. The first involved observing existing problems with privacy practices based on currently used privacy practices in the B2C e-/m-service context, and the second approach involved a survey to obtain the perspectives of both e-service customers and ESP managers. The purpose of the survey was to gain deeper insights into current privacy practices and issues. To understand the customer viewpoint, a questionnaire that included both open- and closed-ended questions was distributed to 53 recruited undergraduate students because online users are likely to be younger and better educated than the general population. To gain the perspective of ESPs, either on-site or telephone interviews were employed using 5 practitioners in the e-service setting.

We drew on a literature review, mainly related to e-/m-/u-services, social contract theory, online behavior and privacy. This literature allowed us to gain insights into the mental frame of ESPs and customers in e-/m-/u-service contexts and the cross-section of customers who are likely to be reached by service providers.

3.2. Instrument development

In our study, a cross-sectional survey was employed. Relevant studies were thoroughly reviewed to ensure that a comprehensive list of measures was included. Except for proactive privacy governance, the majority of the scale items were adopted from the existing literature but were adapted to the privacy and u-service setting of our study. The proactive privacy governance measures were newly developed, and the concepts were derived from ISCT, FIP and a previous study conducted by Challagalla et al. [6]. The measures for perceived u-service value (with emotional, social, and functional dimensions) were derived from previous studies [39,44]. While the concept of value-added strategies was derived from ISCT and Porter [33,34] and the related measures were derived from prior studies [7,23,37], the measures for disclosure willingness were tailored from Dinev and Hart [14]. All scales were slightly modified to adapt them to the research context (i.e., privacy governance in e-services and u-services).

The initial survey questionnaire consisted of three sections. The first section provided concise instructions and definitions of proactive privacy governance, e-services and u-services. The second section consisted of 6 questions that collected demographic information on the subjects (e.g., gender, related experiences on e-services). The last section recorded the subject’s perception of each variable in the model. All key constructs were measured using multiple items and seven-point Likert scales with anchors from 1 “strongly disagree” to 7 “strongly agree”.

Our preliminary instrument was pre-tested through continuous discussion in conjunction with personal interview with 5 faculty members, 4 doctoral students and 7 graduate students who were asked to verify the completeness, wording, and appropriateness of the instruments as well as to confirm the validity of the content. The discussion and interviews enabled the researchers to gauge the clarity of the tasks, assess whether the instrument was capturing the desired phenomena, and verify the important aspects that had not been omitted. The instrument was revised through several iterations, and the review process continued until no further modifications to the questionnaire were needed. Some questions were eliminated or modified because they were found to represent essentially the same aspects as other questions with only slight wording differences. In the end, the self-administered questionnaire comprised 36 items measuring eight latent variables.

3.3. Sampling and survey administration

Data for the study were collected from the B2C e-service setting. Participants needed to be familiar with e-services and have prior experience receiving promotion advertisements via mobile communication devices (e.g., cellular phone, smart phone) because

![Fig. 1. Conceptual model for proactive privacy practices from traditional e-services extending to u-services context. Note: PPG and PV were tested as second order constructs.](image-url)
such users may be more aware of both the positive and the negative potential of u-services at this early stage. The net effect of these characteristics skews the sample population from the general population to a younger, more educated demographic since online users are likely to be younger and better educated than the general population. Prior studies [50,51] have contended that students meet these requirements and that students may even be regarded as the next generation of e-commerce users. Because this study was focused on e- and u-services, online users and undergraduate/graduate students were considered to provide a potential sampling frame, as they reflect the typical customer segment that engages in e-services.

Consequently, participants were not only recruited from online communities (such as Facebook and mail list) but also randomly selected from a pool of students (approximately 950 students) who took information- or management-related courses at four universities in Southern Taiwan. Considering that u-services are still at an early stage, participants may have no comprehensive knowledge about u-services; therefore, before administering the questionnaire, all the participants were required to view a short video that presented some applicable scenarios, such as shopping and using a tour guide. In total, 387 questionnaires were received. Data from respondents who gave incomplete or invalid answers were excluded to assure construct validity. Sixty-three questionnaires were rejected, and the remaining 324 valid questionnaires (213 from campuses and 111 from online communities) were used for the statistical analysis. The potential non-response bias was assessed by comparing the students with the online respondents based on several demographic characteristics (gender, experience with using e-services, providing false information online, and reading privacy policies before using e-services). The Chi-square ($\chi^2$) test was used to examine the distributions between these two groups. No significant differences were observed ($p > .05$). Thus, the research participants who responded to the survey did not appear to compose a biased sample. The details are illustrated in Table 1.

### 3.4. Safeguards against and assessment of common method variance

As self-reported data from a single source were used, common method variance (CMV) might be a potential threat to the validity of the study. Hence, the following three strategies were adopted to safeguard against and evaluate the possible severity of CMV.

1. Several procedural safeguards were applied, such as the use of an anonymous questionnaire with some reversed items, concise and clear items, administering scale length, and three questionnaire sections with separate covers [32].

2. Harmon's single-factor test was used to assess CMV. As expected, no single factor emerged, and eight factors were extracted, collectively accounting for 72.3% of the variance in the data, with the first factor accounting for 20.0% of the total variance. These findings suggest that common method bias is not a major concern.

3. The empirical study validated the research model by using triangulation, beginning with a convergent interviewing, followed by Harmon's single-factor test, and ending with SEM model building and model validation.

### 3.5. Analysis methods

Partial least squares (PLS)—a second-generation structural equation modeling technique—was used to assess the measurement model and then to test the hypothesized structural model regarding its ability to handle formative constructs and highly complex predictive models. This approach was chosen because PLS utilizes component-based estimation, maximizing the variance explained in the dependent variable, and does not require multivariate normality of the data. Furthermore, it imposes less requirements on the sample size, unlike other structural equation modeling (SEM) methods, such as Linear Structural Relationships (LISREL), which is recommended for confirmatory analysis and

---

**Table 1**

Sample demographics.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Classification</th>
<th>Total</th>
<th>Early respondents</th>
<th>Late respondents</th>
<th>$\chi^2$ (Sig.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Male</td>
<td>200</td>
<td>61.7</td>
<td>132</td>
<td>60.2</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>124</td>
<td>38.3</td>
<td>81</td>
<td>38.0</td>
</tr>
<tr>
<td>Experience on e-services</td>
<td>Less than 1 year</td>
<td>48</td>
<td>14.8</td>
<td>30</td>
<td>14.1</td>
</tr>
<tr>
<td></td>
<td>1 – less than 2 years</td>
<td>41</td>
<td>12.7</td>
<td>29</td>
<td>13.6</td>
</tr>
<tr>
<td></td>
<td>2 – less than 3 years</td>
<td>34</td>
<td>10.5</td>
<td>23</td>
<td>10.8</td>
</tr>
<tr>
<td></td>
<td>3 – less than 4 years</td>
<td>26</td>
<td>8.0</td>
<td>18</td>
<td>8.4</td>
</tr>
<tr>
<td></td>
<td>Above 4 years</td>
<td>175</td>
<td>54.0</td>
<td>113</td>
<td>53.1</td>
</tr>
<tr>
<td>Read privacy policy before consuming or registering</td>
<td>Ignore</td>
<td>71</td>
<td>21.9</td>
<td>47</td>
<td>22.1</td>
</tr>
<tr>
<td></td>
<td>Read it roughly</td>
<td>190</td>
<td>58.6</td>
<td>126</td>
<td>59.2</td>
</tr>
<tr>
<td></td>
<td>Read a little in the beginning, then ignore the rest</td>
<td>30</td>
<td>9.3</td>
<td>20</td>
<td>9.4</td>
</tr>
<tr>
<td></td>
<td>Read thoroughly</td>
<td>33</td>
<td>10.2</td>
<td>20</td>
<td>9.4</td>
</tr>
<tr>
<td>Provided false info. online</td>
<td>Yes</td>
<td>251</td>
<td>77.5</td>
<td>167</td>
<td>78.4</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>73</td>
<td>22.5</td>
<td>46</td>
<td>21.6</td>
</tr>
<tr>
<td>Consume online per month (monthly fee exclude)</td>
<td>Less than 200 (NT$)</td>
<td>122</td>
<td>37.7</td>
<td>87</td>
<td>40.8</td>
</tr>
<tr>
<td></td>
<td>201–600</td>
<td>61</td>
<td>18.8</td>
<td>44</td>
<td>20.7</td>
</tr>
<tr>
<td></td>
<td>601–1000</td>
<td>44</td>
<td>13.6</td>
<td>30</td>
<td>14.1</td>
</tr>
<tr>
<td></td>
<td>1001–1400</td>
<td>22</td>
<td>6.8</td>
<td>14</td>
<td>6.6</td>
</tr>
<tr>
<td></td>
<td>1401–1800</td>
<td>14</td>
<td>4.3</td>
<td>6</td>
<td>2.8</td>
</tr>
<tr>
<td></td>
<td>1801–2200</td>
<td>21</td>
<td>6.5</td>
<td>10</td>
<td>4.7</td>
</tr>
<tr>
<td></td>
<td>Above 2201</td>
<td>40</td>
<td>12.3</td>
<td>22</td>
<td>10.3</td>
</tr>
<tr>
<td>Consumed in the past 1 year</td>
<td>Yes</td>
<td>245</td>
<td>75.6</td>
<td>159</td>
<td>74.6</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>79</td>
<td>24.4</td>
<td>54</td>
<td>25.4</td>
</tr>
</tbody>
</table>
requires a more stringent adherence to distributional assumptions [9].

Because of the aforementioned reasons, SmartPLS 2.0 [35] was applied to the data analysis. The two-stage approach was applied to estimate moderating effects, particularly when the formative second-order constructs were involved. Thus, the latent variable scores were initially estimated and subsequently used as indicators in a separate higher-order structural model analysis [22,46]. The model fit was also evaluated using a two-phase approach, i.e., a measurement model and a structural model. In the measurement model, the psychometric properties of all scales were first assessed through a confirmatory factor analysis (CFA). This step was used to assess the reliability and validity of the measurement model and to test whether the empirical data conformed to the presumed model. Then, the structural relationships were validated using bootstrap analysis.

4. Data analysis and results

4.1. Measurement model assessment

To validate the measurement model, its acceptability was assessed by determining the reliability of individual items, the internal consistency between items and the model’s convergent and discriminant validity. Items that shared a high degree of residual variance with other items in the instrument were eliminated from further analysis. After the initial analysis, all items were higher than the threshold value of 0.7, thus indicating a high level of reliability and validity [21]. As shown in Table 2, the loadings for all constructs with reflective measures were well above the recommended cutoff and statistically significant at the 0.001 level, indicating that item reliability for the reflective measures was satisfactory.

Table 3 shows the composite reliability, average variance extracted (AVE), and square root of the AVE, as well as the correlations between the constructs. The composite reliability values of all the constructs were above the recommended level of 0.70, indicating that the internal consistency was adequate [21]. Convergent validity is demonstrated, as the AVE values for all the constructs were higher than the suggested threshold value of 0.50. Comparing the square root of the AVE (bold figures on the diagonal) with the correlations among the constructs, the results indicate that each construct shares a larger variance with its own items than with those of the other constructs, thus indicating that the discriminant validity was adequate [9,21]. However, some of the coefficients were relatively high, so the tolerance values and variance inflation factor (VIF) values were further computed to test for any possible problems with multi-collinearity. A VIF value greater than 4.0 may indicate problems with multi-collinearity, while a VIF value greater than 10.0 indicates serious problems with multi-collinearity. The resultant VIF values (i.e., between 1.46 and 2.71) were well below 4.0, and the tolerance values (i.e., between 0.37 and 0.69) were also greater than 0.2 [21]. The results illustrate that all of the constructs are acceptable and that multi-collinearity is not an issue for the study.

4.2. Structural model assessment and hypothesis testing

A boot-strapping procedure with replacement using 500 subsamples was used to estimate the statistical significance of the parameter estimates shown in Fig. 2. The structural model was examined, and the effects among those latent constructs were also tested. Before testing the interactions among the three independent variables (PPG, PV, and VS), the direct effects of each of the independent variables on customers’ willingness to disclose their personal information were tested in model 1 (main effect model); the results are shown in Table 4. As hypothesized, the paths from proactive privacy governance (H1), perceived u-service value (H2) and value-added strategies (H3a) to disclosure willingness were found to be positive and highly significant. Hypotheses H1, H2 and H3a were all supported, and model 1 explained 31.9% of the variance in customers’ disclosure willingness.

Following Porter’s [33,34] description of competitive advantage as the way that an organization’s activities fit with and strengthen one another and Venkatraman’s [45] guidelines for ensuring correspondence between theory and tests for fit, the hypotheses among the three independent variables (PPG, PV, and VS) on disclosure willingness were assessed using moderation analysis in the structural model by creating two standardized interaction terms, namely, PPG × VS and PV × VS, as examined in model 2 (i.e., interaction model). The interaction model explained 34.3% of the variance in customers’ willingness to disclose their personal information. The results are also shown in Table 4.

The significance of the interaction terms and the effect size, $\beta$, determines the utility of the interaction model over the main effect.

Table 3

<table>
<thead>
<tr>
<th>Construct</th>
<th>Composite reliability</th>
<th>AVE</th>
<th>DW</th>
<th>Emo</th>
<th>Fun</th>
<th>PE</th>
<th>PMFS</th>
<th>PPP</th>
<th>So</th>
<th>VS</th>
</tr>
</thead>
<tbody>
<tr>
<td>DW</td>
<td>0.90</td>
<td>0.65</td>
<td>0.81$^a$</td>
<td>0.84</td>
<td>0.85</td>
<td>0.85</td>
<td>0.85</td>
<td>0.84</td>
<td>0.81</td>
<td>0.81</td>
</tr>
<tr>
<td>Emo</td>
<td>0.92</td>
<td>0.70</td>
<td>0.44</td>
<td>0.63</td>
<td>0.22</td>
<td>0.79</td>
<td>0.69</td>
<td>0.69</td>
<td>0.81</td>
<td>0.81</td>
</tr>
<tr>
<td>Fun</td>
<td>0.88</td>
<td>0.72</td>
<td>0.34</td>
<td>0.28</td>
<td>0.27</td>
<td>0.79</td>
<td>0.69</td>
<td>0.69</td>
<td>0.81</td>
<td>0.81</td>
</tr>
<tr>
<td>PE</td>
<td>0.93</td>
<td>0.72</td>
<td>0.38</td>
<td>0.26</td>
<td>0.25</td>
<td>0.66</td>
<td>0.69</td>
<td>0.69</td>
<td>0.81</td>
<td>0.81</td>
</tr>
<tr>
<td>PMFS</td>
<td>0.92</td>
<td>0.70</td>
<td>0.34</td>
<td>0.26</td>
<td>0.27</td>
<td>0.79</td>
<td>0.69</td>
<td>0.69</td>
<td>0.81</td>
<td>0.81</td>
</tr>
<tr>
<td>PPP</td>
<td>0.90</td>
<td>0.65</td>
<td>0.17</td>
<td>0.27</td>
<td>0.25</td>
<td>0.66</td>
<td>0.69</td>
<td>0.69</td>
<td>0.81</td>
<td>0.81</td>
</tr>
<tr>
<td>So</td>
<td>0.91</td>
<td>0.72</td>
<td>0.34</td>
<td>0.56</td>
<td>0.56</td>
<td>0.16</td>
<td>0.14</td>
<td>0.14</td>
<td>0.85</td>
<td>0.81</td>
</tr>
<tr>
<td>VS</td>
<td>0.88</td>
<td>0.65</td>
<td>0.51</td>
<td>0.53</td>
<td>0.54</td>
<td>0.39</td>
<td>0.42</td>
<td>0.32</td>
<td>0.37</td>
<td>0.81</td>
</tr>
</tbody>
</table>

$^a$ Average variance extracted (AVE).

$^b$ Diagonal elements are the square roots of AVE. Off-diagonal elements are correlations among constructs. For discriminant validity, diagonal elements should be larger than off-diagonal elements.
model. Thus, Cohen’s [12] effect size formula was used to verify the merit of the interaction term that was added to the model. Regarding the overall effect size for the interaction, $f^2$ values of 0.02, 0.15, and 0.35 indicate small, moderate, and large effects, respectively. Chin et al. [10] indicated that a small $f^2$ does not necessarily imply a negligible effect: “Even a small interaction effect can be meaningful under extreme moderating conditions: if the resulting beta changes are meaningful, then it is important to take these situations into account” (p. 211).

$$f^2 = \frac{R^2_{\text{model with moderator}} - R^2_{\text{model without moderator}}}{1 - R^2_{\text{model with moderator}}} = \frac{0.343 - 0.319}{1 - 0.343} = 0.037$$

In this study, the interaction model has an effect size of 0.037, which is between a small and medium effect. As shown in Table 4, the interaction model resulted in slightly higher standardized path coefficients for H1 and H2 (i.e., beta changes). Value-added strategies do have a role to play. Evidently, the interaction between PPG and VS (H3b) had a significant positive impact on DW. Thus, H3b was confirmed. The PV × VS interaction, however, had a negative effect on customers’ disclosure willingness; hence, H3c was partially supported in our study.

### Table 4

<table>
<thead>
<tr>
<th>Independent variable (Path/Beta coefficient)</th>
<th>Direct effect</th>
<th>Moderating effect</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: PPG → DW</td>
<td>0.137 (2.40)</td>
<td>0.176 (3.26)</td>
<td></td>
</tr>
<tr>
<td>H2: PV → DW</td>
<td>0.226 (3.87)</td>
<td>0.231 (4.11)</td>
<td></td>
</tr>
<tr>
<td>H3c: VS → DW</td>
<td>0.130 (4.67)</td>
<td>0.299 (4.28)</td>
<td></td>
</tr>
<tr>
<td><strong>Interactions</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H3b: PPG × VS → DW</td>
<td>0.164 (1.97)</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>H3c: PV × VS → DW</td>
<td>-0.111 (2.02)</td>
<td>Partially supported</td>
<td></td>
</tr>
</tbody>
</table>

$R^2 = 0.319$ 0.343

---

5. Discussion and conclusion

In examining proactive privacy practices for ESPs, we provide various solutions that ESPs can employ to interact with their customers through their privacy practices. In addition, we show how the interplays within the ESP’s proactive approach affect customers’ willingness to disclose the personal information needed for future u-services. This study seeks to provide a theoretical framework that embraces two ideas: (1) ESPs should inform customers of their proactive privacy governance, u-service value and value-added strategies to enhance customers’ disclosure willingness and thus expand their future u-services rather than merely post their privacy policies on their websites. (2) The study was quite ambitious in trying to model relationships at a high order of abstraction and provides some preliminary evidence to illustrate that value-added strategies do indeed matter. While an ESP’s value-added strategies may enhance the positive effect of proactive privacy governance on customers’ disclosure willingness, value-added strategies may also decrease the impact of perceived u-service value on customers’ disclosure willingness. Empirical support for these ideas represents two distinctive theoretical contributions.

The first, more distinctive contribution of this study is the finding that ESPs’ proactive privacy practices enhance customers’ disclosure willingness. Consistent with the hypotheses (H1, H2 and H3a), the results indicate that proactive privacy governance, perceived u-service value and value-added strategies have positive and highly significant direct effects on customers’ disclosure willingness. Notably, the three proposed proactive privacy practices (i.e., proactive provision and protection, proactive education, and proactive monitor and feedback seeking) are important elements of proactive privacy governance in the e-service context. By using these practices, ESPs can alleviate customers’ privacy concerns and thus convince them to reveal their personal information. Similarly, the emotional, social, and functional dimensions of perceived value all significantly contribute to customer perceived u-service value, indicating that the intrinsic value of u-services plays an important role in customers’ disclosure willingness.

Value-added strategies have an extremely strong impact on customers’ disclosure willingness. Evidently, in the e-service context, ESPs’ reputation, incentives, and personalized and alliance-based services affect customers’ decisions regarding
personal information disclosure. This finding is consistent with many prior studies. For instance, while several studies [25,28] have indicated that business reputation can mitigate the effects of information asymmetry, build customer trust and foster customers’ disclosure willingness, many scholars [3,11,28,31] have argued that providing personalized services is the most effective strategy for enterprises to persuade customers to disclose their personal information. Meanwhile, the impact of incentives on customers’ disclosure willingness is consistent with previous studies, which have found that gifts, rewards or discounts are indeed able to motivate customers to share their personal information [8,23,42]. The effect of alliance-based services on customers’ disclosure willingness found in existing studies [7] was empirically confirmed in this study as well.

The second contribution of this study is the finding that value-added strategies significantly and positively affect the effect of proactive privacy governance on customers’ disclosure willingness (H3b). This finding is consistent with Porter’s [33,34] argument that an organization’s activities should reinforce one another to increase the organization’s competitive advantage. The value-added strategies here could be viewed as a type of strategic positioning, which perform different activities from those of their competitors’ or perform similar activities in different ways. Dissimilarity in operational effectiveness among businesses is pervasive. Compared to its competitors, if an ESP uses more comprehensive and effective strategies, customers may consider the ESP to be better at business operations thus to adopt better privacy governance. Thus, considering the benefits and assurances (i.e., value-added strategies) that ESPs/USPs can offer, customers will choose the superior one while the privacy governance is essential and proactively presented to them. Even with a small-to-moderate effect size, our results help to elucidate the conditions under which value-added strategies become a dominant factor in determining customers’ disclosure willingness and when they potentially overshadow the effect of perceived u-service value. For people who are strongly influenced by perceive value-added strategies, perceived u-service value will be a less important factor in whether they decide to disclose their personal information than value-added strategies. If there is a reasonable likelihood of encountering such a group, being aware of this interaction becomes important.

5.1. Theoretical implications

Past research on information privacy in the IS domain has devoted much attention to the beliefs of individuals (i.e., privacy concerns, trust, and risk), representations of privacy policies and privacy seals, relevance of information and calculations of privacy risk [1,3,8,19,23,25,29,48,50,51]. Yet, rarely do studies focus on identifying proactive privacy practices that can guide ESPs in interacting with their customers instead of merely placing their complicated privacy policies in prominent places on their websites. This lack of consideration of the bounded rationality of individuals in research on information privacy is problematic, as information asymmetry will prevent customers from disclosing their information or even motivate them to falsify their personal information, which direct affects customer-provider relationships and thus overall ESP performance.

Drawing on ISCT, this study theoretically and empirically presents a systematic exploration of the proactive privacy practice model. In focusing on the transition of ESPs from providing e-services to providing u-services, this study offers a number of unique contributions to the literature on customer privacy issues related to e-services. First, in focusing on proactive privacy practices for ESPs, this study has not only theoretically constructed a proactive privacy practice model based on ISCT but also revealed some consumer behavior patterns across two contexts (i.e., e- and u-services). This study provides empirical support for the proactive privacy practices that an ESP can implement to encourage its customers to disclose their personal information. It is believed that one of the major contributions of this study is the inclusion of PPG and the simultaneous consideration of the u-service context in the proposed PPPM. To the best of our knowledge, this is the first study in which both issues were systematically examined and explained in the nomological network of information disclosure. As expected, there is evidence that PPG significantly and positively influences customers’ disclosure willingness in future u-services. Hence, PPG can be recognized as an important antecedent of information disclosure.

The second contribution of this study stems from its context: as mentioned previously, many studies have investigated various factors related to information privacy practices, but these studies have generally focused on the e- or m-service context. Considering that u-services may be the next wave in e-commerce, as initiated by e-services and further propagated by m-services [26], the authors focused on both the e-service and the u-service context in this study. Based on bounded rationality and the core assumptions in ISCT, this study argues that an ESP should have responsibilities and obligations to take different relevant actions to interact with its customers in both the e-service and the u-service context. With this in mind, while three proactive privacy practices (i.e., PPP, PE, and PMFS) were to facilitate ESPs’ interaction with customers in the e-service context, ESPs must proactively inform customers of their u-services to communicate the inherent value of their u-services and their value-added strategies. Accordingly, this study proposes a stronger comprehensive theoretical framework, the PPPM, to investigate the underlying factors affecting customers’ disclosure willingness. Since individuals retain the right to participate in economic communities that reflect their own values to the maximum extent possible, individuals will naturally participate in economic communities that reflect their personal and cultural values [15,16]. In summation, the PPPM was proposed to provide the moral fabric for ESPs in the e- and u-service context.

5.2. Managerial implications

Customer information is increasingly being solicited by businesses to improve products or services offered in order to quickly respond to competition in a dynamic marketplace. Unfortunately, as illustrated in the demographic statistics in Table 1, more than three-fourths of the respondents had previously provided fake information online. This result is consistent with prior studies, which have reported that a large percentage of customers withhold or falsify their personal information to protect their privacy [28,29]. Customers’ disclosure behavior thus impedes enterprises’ ability to grow their business into a new vision/stage and establish more intimate customer relationships. Customers’ disclosure behavior is more serious for ESPs, particularly as they try to extend their services/products into the u-service context. For example, targeted customers can be reached by overcoming spatial and temporal restrictions through mobile communication devices, which allow ESPs to provide personalized services to customers through u-services. Diverse personalized services can be provided in a timely manner. If a customer has provided false information to an ESP, the ESP will fail to reach its targeted customer at the right time and the right place even though s/he is in the context-aware, u-service environment.

About 21.9% and 67.9% of the respondents indicated that they usually ignore or only roughly/partially read, respectively, the relevant privacy policies of websites. These results are consistent with confirmed those of previous studies [2,28,42]. Because
privacy policies are always too complex to understand, online customers rarely make the effort to read them. Without sufficient knowledge of ESPs’ privacy policies, customers with have greater privacy concerns and avoid registering or transacting online. In this study, personal interviews were conducted either on-site or by phone to gain deeper insights into the results and the behavior of both customers and ESPs. The interviewees included six practitioners (two from the most popular international auction websites, three from famous communication network companies and one from a company that helps customers develop e-service websites), four scholars and six undergraduate students who were familiar with and had used e-services. Some gaps between consumers and practitioners were explored through the interviews that are subsequently elucidated.

Most of the practitioners argued that they have comprehensive privacy practices to protect customers from privacy threats and that privacy invasions are generally caused by customers themselves, by improperly using the systems, recklessly downloading files, and so forth. Conversely, the customers stated that privacy invasions result from the ESPs, as a result of the unauthorized dissemination of personal information, junk mail and advertising messages. After customers clicked the “I agree” button and submitted the “terms and conditions” for using the e-service, ESPs considered customers to have authorized the use of their personal information. However, most customers rarely read “terms and conditions” and just click “I agree” if they indeed need online services or products.

Traditional approaches to management that may have been effective in a booming economy are no longer sufficient to satisfy the demands of a changing marketplace. People provide false information merely because they have a limited or no understanding of how ESPs use their information. Thus, ESPs must proactively and comprehensively communicate the important and valuable information (e.g., utilities and benefits from u-services, assurances for and monitoring of customer information usage, and redress for privacy invasion) related to their e-services to customers. For example, such information should be provided in a simple, precise and salient format with registration forms rather than via a “link” to various complex policies, such as “terms of services” or “privacy policy”, which are only presented as checkbox items stating “I agree to the Terms of Services and Privacy Policy” or “I do not agree …”. Therefore, valuable and workable alternatives are delineated below.

Regarding proactive privacy practices in an e-service context, the results suggest that the PPPM provides effective and efficient guidelines for ESPs to use in interacting with customers in order to increase customers’ trust in ESPs, to eliminate or minimize conflicts and gaps in knowledge regarding privacy practices, and alleviate privacy concerns in the e-service context as well as foster customers’ disclosure willingness in future u-services. Given the significant consequences of the PPPM, some suggestions are proposed. First, ESPs are advised to initiate interactions with their customers by use the proposed three practices related to PPG in order to convey relevant information with respect to privacy assurance, remedies, customer rights, obligations and protection practices, especially those related to u-services. ESPs can also learn more about their customers by seeking customer feedback, which may trigger service/product innovations and also enhance customer satisfaction and retention.

As another proactive practice in the e-service context, ESPs are advised to inform customers of the advantages that they may gain from adopting u-services. The more benefits that a customer perceives from u-services, the more likely a customer will be willing to disclose his or her personal information. U-services are at an early stage, and most people are thus unfamiliar with u-services. Privacy concerns might thus outweigh the benefits of u-services. Therefore, ESPs would benefit from comprehensively explaining the value of u-services to their customers, which may increase the customers’ perceived value of u-services. Finally, it is advisable that ESPs develop strategic methods to reinforce or motivate customers to disclose their personal information. For instance, ESPs may consider offering benefits, such as coupons or discounts, or providing personalized and alliance-based services to customers in return for their personal information. An ESP’s reputation can also enhance customer trust and thus customers’ disclosure willingness in future u-services.

5.3. Limitations

This study started by discussing integrative social contracts theory and proposed a concept model to explore the sophisticated causal relationships between ESPs’ proactive privacy practices and customers’ disclosure willingness. However, this study is not without certain limitations, which represent opportunities for further research. First, this study was conducted in Taiwan and is based on a single sample. The usual caveats concerning the use of single informants and self-reported data apply to this study, and therefore, some caution is advised when generalizing the findings. Further studies might need to expand the boundaries of the analysis to other populations. Moreover, exposure to u-services is limited, as u-services are still at an early stage. Most people lack any real experience in using diverse u-services and have insufficient understanding of the applications of u-services, which may be cause for concern. Finally, the proposed model variables explained 34.3% of the variance in customers’ disclosure willingness. Although such an approach was not adopted in this study, it may also be of interest to use a more fine-grained approach (e.g., using customer characteristics, situation-specific variables) in concert with the higher level analysis conducted in this study to examine other relationships that were not explored between the first-order constructs. For example, future research may examine whether perceptions of privacy risk and trust at the first-order level are interrelated to customers’ disclosure willingness.

6. Conclusion

Businesses constantly aim to establish more intimate customer relationships. Because customer information is imperative for enterprises to gain a competitive advantage in today’s dynamic marketplace, u-services have recently received great attention, and they may be at the core of future business models. This study contributes to an emerging stream of research on proactive privacy practices by providing an original theoretical explanation for how ESPs’ proactive privacy governance and customers’ perceptions of u-service value interact with ESPs’ value-added strategies in influencing customers’ disclosure willingness. Since only a few experimental u-service prototypes have been developed by certain universities in Taiwan, u-services are at an early stage. With the high proportion (77.5% in this study and 63% in Kobsa’s [28] work) of respondents having previously provided false information on websites, an effective solution communicating privacy practices to encourage information disclosure is pressing at this early stage. Drawing on ISCT and examining proactive privacy practices for ESPs, this study proposed the PPPM, which allows ESPs to strategically manage consumer information and leverage privacy protection to gain a competitive advantage. The PPPM also helps ESPs identify the strengths and weaknesses of their current privacy practices, to help ESPs develop more proactive and effective privacy practices in extending their business toward u-services or u-businesses.
Acknowledgments

This research was supported by the National Science Council of Taiwan, under operating grants NSC 99-2410-H-110-045-MY3 and NSC 100-2410-H-022-003-MY2. It was also partially supported by the Aim for the Top University Plan of National Sun Yat-Sen University and the Ministry of Education, Taiwan.

References