Understanding the Effect of Privacy Concerns on User Adoption of Identity Management Systems

Ali Alkhalifah\textsuperscript{1*}, Sulaiman Al Amro\textsuperscript{2}

\textsuperscript{1} Information Technology Department, Computer College, Qassim University, Qassim, Saudi Arabia.
\textsuperscript{2} Computer Science Department, Computer College, Qassim University, Qassim, Saudi Arabia.

* Corresponding author. Tel.: +966163801730; email: a.alkhalifah@qu.edu.sa
Manuscript submitted November 12, 2015; accepted December 29, 2015.
doi: 10.17706/jcp.12.2.174-182

Abstract: Privacy concerns are one of the most important issues in today's technology-based setting. Previous studies show that privacy concerns negatively influenced the individual's behavioral intention toward a particular Web-based service or technology. However, researchers have not explored the role of privacy concerns in identity management systems (IdMS) adoption. Previous identity management studies addressed privacy issues from the technical perspective but theoretical, social and regulatory dimensions have not been well addressed in the literature. This study identifies multi-dimensional privacy concerns of the IdMS and aims to understand and examine their effect toward users behavioral intentions to adopt IdMS. The conclusion of this paper outlines the implications and further directions for this study.

Key words: Behavioral intention, identity management systems, identity information, privacy concerns.

1. Introduction

Online users have serious privacy concerns about how their personal and sensitive information is used, protected, disclosed in addition to the degree of control they have over the dissemination of this information [1]. Furthermore, they are concerned about possible undesirable social effects resulting from the abuse of such information. In fact, 88.2% of Internet users express concern about the privacy of their personal information [1], and research has shown that privacy of information is a crucial concern for individuals [1]-[3]. Many researchers have argued that information privacy, with related user concerns, is one of the most important issues in today’s technology-based setting [4], [5]. Moreover, privacy is a major concern when online consumers engage in transactions [6]. Concern about privacy has co-evolved with advances in information technology (IT) as businesses have begun to use the Internet for sharing and exchanging personal information. The term, privacy concern, refers to the sense of anxiety that persons have because of a variety of possible threats to the person's right to freedom from privacy invasion [7]. Users feel that they are in danger when technology has the capability to retrieve, store and communicate their personal information [8]. Although some studies examined online privacy among Internet users [2], [7], few studies have provided a theoretical framework on the specific nature of information privacy concerns [3], [5], [7].

Threatening behaviors in the online world are also on the rise, particularly those associated with identity theft. Identity theft significantly affects the economic decisions that people make [9] and poses security risks targeting both organizations and individuals [10], [11]. Identity Management Systems (IdMS)
represent solutions that are employed to manage end-user authentication, access rights and restrictions, account profiles and other attributes that provide an individual with more control over his/her identity information [12]. The goal of IdMS is to foster productivity and security while lowering the costs related to managing users and their identities, credentials and attributes. Privacy concerns are most important issues related online identity management and IdMS [13], [14]. The implementation of new IdMS entails new risks. Thus, understanding how the risks arising from new IdMS deployed in online service are perceived and addressed may be critical to individual acceptance of online services [14]. However, little is known about how users perceive the use of IdMS. Therefore, it is critical to understand IdMS users’ concerns for information privacy to maximize the potential of IdMS as well as online services.

Previous identity management studies addressed privacy issues from a technical perspective [15], [16]. Theoretical, social and regulatory dimensions have not been well addressed in the literature [17]. Many identity management researchers suggest that privacy concerns as well as the relationship among them should be investigated and formulized [14], [17]-[19]. Privacy concerns have been viewed as antecedent beliefs, which influence users' behavioral intention toward using a particular technology. The majority of prior studies that examines the influence of privacy concerns on individual behaviour typically tests them as a single construct [5], [20], [21]. There is a lack of studies that investigate and test privacy concerns as a multi-dimensional construct [4] and individual behavioural intention toward IdMS. This paper aims to fill these gaps and examines users' privacy concerns and their effect on users' behavioral intention to adopt IdMS. This paper focuses on three inter-related issues. First, it identifies factors that affect user adoption of IdMS. Second, it theoretically examines and defines the dimensionality of privacy concerns and their importance in predicting users’ behaviors in the context of IdMS. Thirdly, it proposes a model to examine user adoption of IdMS centering on privacy concerns.

The current study extends the body of research by studying multi-dimensional privacy concerns including concern for information privacy (CFIP) [22] and Internet users’ information privacy concerns (IUIPC) [7] measures consisting of seven dimensions: errors, collection, improper access, secondary use, control, choice, and awareness. We believe that this approach contributes to IdMS and information systems literature relating to privacy and emerging IT artefact adoption. IdMS providers and designers face the challenge of creating security and privacy polices [14], [23] in an environment that resists adoption, especially at the individual level [13]. The proposed framework practically would offer an increased understanding of user’s privacy concerns, which in turn will provide designers with a tool that can be used to develop trust strategies that will encourage IdMS adoption.

The rest of the paper is organized as follows. Section 2 provides an overview of IdMS. Section 3 introduces and defines privacy concerns. Section 4 discusses the model proposed in this study. Section 5 describes the research methodology. The final section provides a conclusion and discusses future research directions.

2. Identity Management Systems

IdMS have been defined as the integration of important personal information from multiple systems into one collaborative and unique identity [24]. This study focuses on Web-based IdMS and defines IdMS as the business processes, polices and emerging technologies, for the creation, maintenance and use of online identities across the Internet and within online service providers. IdMS are services available on the Web that enable users to create and manage their online identity. In the offline world a person carries multiple forms of identification in her or his wallet, such as driver's licence, health insurance card, credit cards, affinity cards such as frequent flyer and loyalty cards. Similarly IdMS enable individuals to create a number of digital
cards which they use to identify themselves with Web services that accept them. If a user subscribes to an identity management service, they can access websites affiliated with the identity management service. The user can manage their identity information among various websites in an integrated way through this service. Examples of IdMS include: Microsoft Passport, OpenID, InformationCard (CardSpace), Facebook Connect, Web Single Sign-on, PayPal Access etc.

The majority of current IdMS studies focused on technical or design problems and challenges of IdMS [15], [16], [25]. Perceptions of online identity and IdMS from individual perspectives have been explored in previous research [13], [14], however no study to date empirically explores and measures factors that may impact the user adoption of IdMS. Moreover, current research indicates that the provision of suitable frameworks or models to better understand IdMS from both business and individual perspectives are equally limited although evidence suggests that individual and business applications are the biggest growth area [13]. There is a lack of studies reported in the academic literature focusing on Web-based IdMS that investigate self-regulation IdMS [17], [18]. Therefore, we believe that the selected scope of the current study focusing on the users’ adoption of IdMS could fill these gaps and contribute to both the IdMS and IS literature.

3. Privacy Concerns

Privacy is defined as “the moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state” (p. 467) [26]. There are reasons for privacy protection: 1) privacy enables people to control their information; 2) privacy is the right to be left alone; 3) privacy can be used as an agent to use and control information collection [8].

A user’s perception of privacy includes an estimation of the possible privacy benefits and risks related to his/her use of IT applications. User’s privacy concerns start from the feeling that his/her information is vulnerable and he/she is not able to control and manage his/her personal information [27]. Hui et al. [27] explored users’ attitudes towards privacy with regard to using an online website and communicating personal data. Their study empirically showed that online users care about how their personal data (including identity data) is managed online. Consistent with expectancy theory, users will perform in ways that maximize positive effects and minimize negative results [20]. Hence, users’ privacy concerns differ, depending on the purpose of using the technology. Therefore, users’ privacy concerns in the context of IT use and adoption are situation dependent [8].

Privacy concern has been shown to directly influence users’ behavioral intentions in a variety of contexts, including e-commerce [7], ubiquitous commerce [8], social networking communities [28], [29], travel websites [5] and security technology [30]. Most of these studies examined privacy concerns as a single construct. Although several researchers have examined individual privacy concerns in various web settings, little is known about how privacy concern affects user behavioral intention to adopt IdMS.

3.1. Privacy Concerns Dimensions

Smith et al. [22] suggested that what drives users’ concerns about information privacy (CFIP) consists of four dimensions: errors, collection, improper access and secondary use. This measure was the first of its kind to measure individuals’ concerns regarding organizational practices. Stewart and Segars [31] argued that these four dimensions can be incorporated into a second-order factor and that CFIP should be developed following advances in technology and research as well as practice. Based on social contract theory, Malhotra et al. [7] found that Internet users’ information privacy concerns (IUIPC) is a second-order factor with three dimensions: control, collection, and awareness. Liu et al. [32] found that the condition of privacy includes notice, choice, access and security. Table 1 summarizes some measures of privacy concern that have been applied in different contexts.
### Table 1. Studies of Privacy Concerns and Their Dimensions

<table>
<thead>
<tr>
<th>Study</th>
<th>Area or Application</th>
<th>Privacy concern</th>
<th>Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>[22]</td>
<td>Organizational practices</td>
<td>Concern for information privacy (CFIP)</td>
<td>Errors (4 items), collection (4 items), improper access (3 items) and secondary use (4 items)</td>
</tr>
<tr>
<td>[7]</td>
<td>Internet</td>
<td>Internet users' information privacy concerns (IUIPC)</td>
<td>Collection (4 items), control (3 items) and awareness (3 items)</td>
</tr>
<tr>
<td>[33]</td>
<td>Internet</td>
<td>Privacy concerns and control techniques</td>
<td>Concerns about unauthorized use (6 items) and concerns about giving out personal information (4 items)</td>
</tr>
<tr>
<td>[32]</td>
<td>e-commerce</td>
<td>Privacy concern</td>
<td>Notice, choice, access and security (all 7 items)</td>
</tr>
<tr>
<td>[20]</td>
<td>Internet</td>
<td>Privacy concerns</td>
<td>Information privacy concerns (4 items)</td>
</tr>
<tr>
<td>[2]</td>
<td>Internet</td>
<td>Privacy concern</td>
<td>Privacy attitude (16 item), privacy behaviour, general caution (6 items), technical protection (6 items)</td>
</tr>
</tbody>
</table>

### 4. Research Model

The conceptual model illustrated in Fig. 1 asserts that behavioral intention is a key variable in determining IdMS adoption and is a function of privacy concerns dimensions. These include collection, improper access, error, secondary use, control, awareness and choice. In the following sections, the dependent variable and these independent variables are identified and discussed, and the relationships among them are explained through the conceptual model and development of the hypotheses.

![Fig. 1. Research model.](image)

#### 4.1. Privacy Concerns Constructs

The literature in consumer privacy highlights that social contract theory (SCT) is appropriate for understanding the tensions between consumers and firms over information privacy [34], [35]. SCT proposes that members of a given industry or community behave fairly if their practices are governed by social contracts [36]. In the context of information privacy, “a social contract is initiated, therefore, when there are expectations of social norms (i.e., generally understood obligations) that govern the behaviour of those involved” [34]. SCT has been used as conceptual tool for understanding and predicting consumer behaviour in the context of information privacy [7], [35]. Malhotra et al. [7] developed Internet users’ information privacy concerns (IUIPC) based on SCT. They argued that “When applied to information privacy, SCT suggests that a firm’s collection of personally identifiable data is perceived to be fair only when the consumer is granted control over the information and the consumer is informed about the firm’s intended use of information” (p. 338).

Privacy concerns, such as CFIP and IUIPC arise as part of the interaction between a user and a provider. Similarly, during user-centric IdMS, the individual’s interests are known in the sense that they manage their own personal data and get credentials from identity providers, which they can use in their interaction with
service providers [37]. In that regard, IdMS users are subject to specific privacy-related risks. Hence, this study adopts the CFIP and IUIPC variables as well as measures developed by Liu et al. [32], which have been identified and demonstrated as being of primary concern to Internet and e-commerce users. Given the similarity in terms of human users interacting with Web systems, we believe that these dimensions offer valuable insights into IdMS users' privacy concerns. For the purposes of this study, privacy concerns are categorized in seven dimensions as follows:

- **Collection**: the perception that too much information is being collected and whether identity information is properly collected.
- **Improper access**: information storage security.
- **Errors**: accuracy of identity information storage in databases.
- **Secondary use**: identity information collected for one purpose is used for other purposes without users' permission.
- **Control**: users are concerned whether they can control their identity information.
- **Awareness**: the degree to which a user is concerned about his/her awareness of information privacy practice.
- **Choice**: users are concerned whether they can select, alter or delete their identity information.

When collecting users' identity information, IdMS providers may require unnecessary information such as identification card number and credit card account. This may raise users' concern about information over-collection. IdMS providers ensure that only those authorized users can access the databases containing identity information. However, they may be unable to prevent hacker attack on and intrusion into the databases. This leads to users' concern about improper access. IdMS may not adopt measures such as verification to ensure information accuracy [38]. This could have a negative effect on the service quality of IdMS and increases users' concern about information errors. IdMS providers may share some information with third parties which hurts users' benefits and brings great privacy risk to them. Users may worry whether their identity information is properly collected, accurately and securely stored, and appropriately used. This raises users' concerns about future potential loss associated with disclosing identity information.

### 4.2. Behavioral Intention

This study proposes behavioral intention as a substitute for actual behavior, and it establishes the importance of behavioral intention as a determinant of the user's adoption of IdMS. Behavioral intention is a measure of the strength of one's intention to perform a specific behavior [39]. Because using IdMS requires users to disclose their personal information in order to manage and control them, both intention to disclose and intention to use must be considered. Thus, we define behavioral intention as a user's intention to disclose her/his identity information and to use an identity management systems service or technology. From a practical perspective, it is worth noting that IdMS are still in an early stage of development in many places [40], [41]. Hence, the choice of behavioral intention rather than actual usage as the dependent variable is considered both necessary and appropriate.

### 4.3. Privacy Concerns and Behavioral Intention

Privacy concern has been viewed directly as a negative antecedent belief, which influences users' behavioral intention and can affect users' attitudes towards using an IT artifact. For any rational decision maker, the decision is made derived from an evaluation of perceived costs and benefits [42]. Rational decision makers are motivated to minimize negative outcomes [8], [20]. Consistent with the theory of reasoned action [43], privacy concerns viewed as a negative antecedent belief, which could influence an individual's attitude and, in turn, affects an individual's behavioral intention [8]. Previous research has
found that privacy concerns can have a negative effect on the adoption of Web-based applications and therefore these concerns are a main threat to e-commerce usage [7]. Dinev and Hart [20] found that consumers’ privacy concerns are negatively associated with their purchases on the Internet and negatively influence the willingness to provide personal information on the Internet. An experimental study on the adoption of ubiquitous commerce [8] also showed that privacy concerns have a negative effect on intention to adopt u-commerce services. Lee and Granage [5] examined how privacy assurance affects privacy concerns and perceived usefulness on travel Websites and identified the role of these outcomes in predicting customer behaviour responses, such as making purchases and willingness to reveal personal information. They noted that by enhancing the privacy assurance, customer privacy concerns are decreased and the perceived usefulness of services is increased. Moreover, their findings indicated that customer behavioral responses are negatively related to privacy concerns and positively associated with the perceived usefulness of the services. Junglas et al. [4] argued that future technology adoption will be less determined by usefulness factors than by concerns that go against human nature. In addition, Crespo and delBosque [44] suggested that it would be interesting to consider consumers’ privacy concerns and trust in Internet-based services and technologies among other variables. In that regard, it would be interesting to determine the most innovative user concern and the cases where privacy concern explains the most significant impacts on future intention to adopt IdMS. Therefore, we hypothesize that: Privacy concern has a negative effect on users’ behaviour intention to adopt IdMS.

5. Research Methodology

The research instrument to measure the constructs of the model was developed by adapting existing measures to the research context. Intention to use measures were adopted from Davis [39] and Venkatesh et al. [45]. Intention to disclose identity information measures were adopted from Belanger and Carter [46] and Fogel and Nehmad [28]. Privacy concerns measures were adopted from Smith et al. [22], Malhotra et al. [7] and Liu et al. [32]. All the variables will be measured on a 7-point Likert scale.

The data collection process will be carried out using an online survey method, and the questionnaire will be Web-based. The participants will be social networkers specifically Facebook and LinkedIn users as well as users who engage in online shopping and use online payment services. The targeted participants were selected because they have experience with online identity services where individuals create online profiles, make connections with others and share identity information. It is decided to collect data from the aforementioned target population to ensure that there would be a sufficient number of potential IdMS adopters in the sample.

6. Conclusion

The objective of this paper is to investigate and develop a model of how multi-dimensional privacy concerns effect users’ adoption of web-based IdMS. Such a model has not been suggested in past literature. From theoretical perspective, this study contributes to IT usage and adoption research by presenting a theoretical model to explain IdMS adoption. In addition, we developed a road map to measure privacy concerns as factors related to the end-users’ potential for IdMS adoption. This study hopefully will stimulate further research and provide a useful lens for examining privacy issues in the context of acceptance of emerging innovative web technology in its early adoption stage. It also contributes to a growing body of literature on the enhancement of web services and mitigating Internet privacy concerns. Designing a privacy-enhancing technology is not just a technological issue, but theoretical, social, and regulatory dimensions must also be addressed [17]. This study understands privacy concerns and identifies factors that must be considered in designing privacy-enhancing IdMS that address online identity management.
This study will be complemented with additional quantitative examination in order to validate the framework by empirical measurement and will test the causal network of correlation in the model using survey instruments. The data will be analyzed using the well-established Structural Equation Modeling (SEM) technique: Partial Least Squares (PLS) to examine relations between the constructs of the conceptual model and to assess the overall fit of the structural model [47].

References


29(4), 393–409).


Ali Alkhalifah received a BS in computer science from Qassim University in 2007, and master (honor) in IT from the University of Newcastle in 2010, and PhD in information systems from the University of New South Wales, Australia in 2013. He is an Assistant Professor in Computer College at Qassim University. Until recently he was the head of IT department. He has been involved in several program committees and is being a Reviewer in different international conferences and journals. Dr. Ali has a number of research interests including e-business, identity management systems, evaluation of the World Wide Web, and the semantic Web.