Toward multi-dimensional trust: exploring antecedents to trust in a complex domain

Alexander McLeod* and Sonja Pippin

Department of Accounting and Information Systems,
University of Nevada, Reno,
1664 N. Virginia St. Reno, NV 89557, USA
E-mail: amcleod@unr.edu
E-mail: sonjap@unr.edu
*Corresponding author

Abstract: This research proposes a new multi-dimension trust model and develops a typology of antecedents to trust in the context of high domain complexity. Using open-ended questions, we explore what users think would create, promote or manage trust. We argue that trust affects individuals' intention to use tax preparation software and electronic tax filing. This is an interesting research setting because of

1. the complexity of the tax law
2. the privacy of the subject matter
3. the omnipresence of the issue
4. the current promotion of e-filing by the Internal Revenue Service
5. individual taxpayers' ambivalence or negative attitude toward taxes and the government.

We propose that when the information system serves as surrogate for a domain expert, multi-dimensional trust and several novel antecedents to trust, such as power and control based, reparative, and system-quality based antecedents should be considered as potential determinants of use.

Keywords: trust; tax preparation software; multi-dimensional trust; trust antecedent model; trust antecedent typology; logic trust; privacy trust; security trust; software creator trust.


Sonja Pippin is an Assistant Professor in the Department of Accounting and Information Systems at the University of Nevada Reno. She received her MS in Geography from the University of Zurich, Switzerland, in 1998. In 2001, she graduated with an MS in Tax from Texas Tech University and in 2006 she earned her Doctorate in Business Administration (Accounting) also at Texas Tech University. She has taught various undergraduate and graduate accounting courses and currently teaches mostly corporate taxation. Her research interests include technology acceptance in the accounting and tax environment, as well as public policy (tax policy) and public finance related issues.

1 Introduction

In this paper, we describe an exploratory study initiated to determine user perceived antecedents to trust. The setting is the complex domain of tax software where individuals prepare and electronically file income tax returns. Tax software in this scenario functions as a surrogate for professional tax preparers. Based on our literature review we propose two constructs which lead to intention to use tax software – trust in the information system and trust in the associated entity, in this case the Internal Revenue Service (IRS). We identify several dimensions of trust required for individuals to accept tax preparation software and e-filing. Next, we use an exploratory open-ended questionnaire to develop antecedents to these constructs for the two-step process of preparing and filing taxes electronically, a complex subject area. Complexity of domain is especially important when information systems serve as a surrogate for a domain expert because users must trust in the information system and the party receiving the output of the system.

Human-computer interaction in the tax return preparation domain is a highly relevant topic in the USA. In 1998, the Internal Revenue Service Restructuring and Reform Act of 1998 (P.L. 105–206) introduced a goal of 80% electronic filing (e-filing) for all federal tax returns by the year 2007 [§2001(a)(2)]. Recent announcements by the IRS indicate that, while this goal will not be reached, the rate of individual e-filing has increased significantly over the past several years. Electronic filing implies the use of new technology, such as the internet and some form of tax preparation software. These types of software packages have been in use for many years by professional accounting firms. With the IRS’s quest to improve the quality of returns and increase the number of individuals e-filing their returns – tax preparation software packages have become available and affordable to the individual taxpayer. Even though most individual taxpayers have accepted and adopted tax software, there remains a group of resistant taxpayers or laggards who are still hesitant to use software and to e-file because of various reasons, such as lack of trust (Wu and Chen, 2005). Furthermore, since the e-filing initiative can be considered as a relatively successful e-government program, proponents of other e-government plans should also be interested in these results.

The context of individual tax preparation is a unique environment because the tax preparation software serves as a surrogate for the professional tax preparer. Most individual taxpayers are not tax experts having limited capabilities to verify system output. Moreover, individual tax preparation can be perceived as a two-step process. First, individuals must choose among using tax software, preparing a tax return by hand, or paying a professional preparer. Second, individuals can file their tax returns either electronically or via regular mail. The relationships between the individual taxpayer, the
software producer, the tax software, and the tax collection agency – the IRS in the USA – are shown in Figure 1.

**Figure 1** Tax preparation relationships

The interaction of these entities through the tax preparation software requires that the individual taxpayer trust
1. the tax domain logic programmed into the software
2. the privacy protection built into the system
3. the security mechanisms involved in protecting the user’s computer and transmission of the return.

In addition, the individual’s trust of the taxing authority receiving and electronically storing the tax information becomes important. The relationships in Figure 1 reveal that two forms of trust are relevant: trust in the information system and trust in the associated entity. This means that research models including simple (i.e., uni-dimensional) trust may be insufficient for complex contexts. We propose that, because of the complexity of the tax domain, trust might be viewed as multi-faceted or multi-dimensional. For the purposes of this work, we define multi-dimensional trust as a situation where trust in a system is required in addition to trust in another entity or person. This leads to the following research questions:

1. In the tax preparation setting, do users need to trust both the system and the entity creating the software?

2. Is trust in an associated entity important in complex domains?

If trust in an information system and other entity is needed in complex environments, then differentiating between different precursors to these forms of trust is important (Kim et al., 2008; Bolton et al., 2008; Dyer and Chu, 2010; Riedl et al., 2010). Prior studies have examined the relationship between antecedents and simple trust in information systems. These antecedents can be categorised into technology-based (Chellappa and Pavlou, 2002), knowledge/experience based (Ba and Pavlou, 2002), and institutional
Understanding what creates and fosters trust is important for academics as well as IT professionals. Domain and environment have long been identified as important determinants of human computer interaction (Butler and Fitzgerald, 1999; King and He, 2006; Liu and Arnett, 2000; Martins and Kellermanns, 2001; Roth and Kostova, 2003; Rudisill, 1996). For example, many studies examine how cultural, organisational, and demographic variables impact the use of information systems (Lippert and Volkmar, 2007; Morris et al., 2005; Straub and Keil, 1997). This paper contributes to the literature by providing a model that illustrates the influence of a specific and relatively complex domain on human-to-human and human-to-computer relationships. Results of the exploratory survey have implications for academics, software creators, and policy-makers.

If the quality of the human-IT interaction depends on an individual’s trust in the system and trust in the relationships, creating and managing the different aspects of trust will improve efficiency and effectiveness of technology use. Individuals may trust the tax software system, the creator of the software and the IRS because of technological features of the software, the software creator’s reputation, or their prior experience using tax software and e-filing. Providing a typology for the various antecedents will help understand these relationships and provide the background for future research. Thus, we ask the following additional questions:

3 What antecedents to trust are important to users in complex environments?
4 What creates, promotes, or manages trust in complex environments?

The remainder of this paper is structured as follows. In the following section, we provide the theoretical background for this research. Section 3 introduces the research model and Section 4 reports the methodology. Section 5 discusses results and Section 6 concludes the paper.

### 2 Theoretical background

The relationship between trust and information system use has been the subject of many academic studies. In general, these studies predominantly focus on e-commerce, online transactions and web purchases (Bunker and Bartholomew, 2010; Chellappa and Pavlou, 2002; Cheung and Lee, 2001; Gefen et al., 2003; Gefen and Straub, 1997; McKnight et al., 2002; Kim and Tadisina, 2010). The relatively high uncertainty and risk involved with e-commerce transactions – compared to ‘traditional’ shopping – drives research in this area. We find that many information systems studies examine trust as single dimension construct (Chen and Tan, 2004; Keat and Mohan, 2004; Nicolaou and McKnight, 2006; Suh, 2003). However, recently several researchers have expanded the concept of trust into a multi-dimensional construct, arguing that the complexity of information system environments requires a more thorough review of the different aspects of trust. For example, Gefen and Straub (2004) synthesise some of the trust dimensions found in prior literature and provide a model that allows for multi-dimensional trust using the four dimensions integrity, predictability, ability, and benevolence. That is, the trust dimensions relate to characteristics of the other individual or entity in the information systems relationship.
Grabner-Kräuter and Kaluscha (2003) differentiate between two forms of trust, interpersonal and impersonal, because in the information systems context human-to-human as well as human-to-artefact interactions take place. Thus, according to them, trust can be differentiated into ‘relationship trust’, defined here as trust between the individual human actors in the system, and ‘system trust’, defined here as trust in the information system. The tax preparation relationship diagram (Figure 1) suggests that this distinction also applies in the tax context.

Prior research has examined individual tax filing and information technology in other countries but not tax preparation. These studies integrate certain aspects of system trust in their models. The authors find that perceived credibility – defined as the individual’s perceived security and perceived privacy protection of the e-filing system – affects individual perception of the efficiency and effectiveness of the system (Chang et al., 2005a; Fu et al., 2006; Wang, 2003). Paul and McDaniel (2004) examine interpersonal trust in a multi-dimension format and its effect on virtual collaborative relationships. They view trust as calculative and integrate three factors; self interest, ability and empathy.

Relationship trust concerns an individual’s trust in the creator of the software and in the associated entity. We distinguish between creator and associated entity because in the tax context it is likely that the technology creator is not the information recipient. In particular, tax preparation software is created by programmers working for different software companies, and the information recipient is the tax collection agency.

The question, ‘what creates trust?’ has been previously asked in studies and various academic disciplines have examined the many antecedents to trust, such as the length of the relationship and the satisfaction with the other entity’s performance (Leisen and Hyman, 2004); the cultural environment (Schoorman et al., 2007); organisational policies (Gould-Williams, 2003); managerial behaviours (Bijlsma and Van De Bunt, 2003); expertise, openness, cooperation, tactfulness, timeliness, sincerity, congeniality and integrity (Ghosh et al., 2001); and institutional structures, individual disposition and experience (Warkentin et al., 2002). Investigations of antecedents of trust in information technology attempt to enhance and improve acceptance and trust in order to reduce transaction costs (Chellappa and Pavlou, 2002; Chellappa and Sin, 2005; McKnight et al., 2003; McKnight et al., 2004; Pavlou, 2003; Pavlou and Dimoka, 2006; Pavlou et al., 2007; Xia et al., 2008). Generally, these antecedents can be categorised as follows:

- technological antecedents, such as password protection, virus scanning software, and firewalls (Chellappa and Pavlou, 2002)
- knowledge or reputational antecedents, such as personal experience, history or referrals by friends with experience (Ba and Pavlou, 2002)
- institutional antecedents such as seals of approval and certifications (Xia et al., 2008; McKnight et al., 2004).

In light of these studies and based on the proposed relationships in Figure 1, we introduce several dimensions of trust measuring an individual’s trust in the information system (‘system trust’), and individual’s trust in the other entities (‘relationship trust’). In other words, users trust the tax software (‘system trust’) and the IRS (‘relationship trust’). Trust in the system is further differentiated into
trust in the software logic
trust in system privacy
trust in system security.

System privacy is defined as the belief that personal information entered into a system will remain private. For example, concerning tax preparation software, a user who trusts the system privacy expects that no personal tax information will be divulged to unauthorised people or systems. System security is defined as the belief that the information system will be safe from hacking and the introduction of viruses. For example, a user who trusts the system security expects to use the system without introducing viruses or other unsafe software effects into their machine. These definitions imply that privacy and security are two interrelated but different concepts. Yet, most information systems research concerning trust does not make this distinction. One notable exception is Chellappa and Pavlou (2002).

The results of prior studies are mixed with regard to the importance and effectiveness of some of the antecedents to trust (Chellappa and Pavlou, 2002). We are not certain that these antecedents or their classifications adequately describe antecedents of trust in the context of tax preparation software where the information technology serves as domain expert.

3 Developing the model

The relationships shown in Figure 1 imply that the system user must trust the system (‘system trust’), the associated entity, and the creator of the system (‘relationship trust’). These constructs correlate with some distinctions made in prior literature (Grabner-Kräuter and Kaluscha, 2003). We refine our model based on the traditional definition of trust by Mayer et al. (1995). This definition suggests that trusting others in a relationship means that there is the potential for physical, emotional, or financial harm when interacting with this entity or system. The users who trust a system must believe that despite the potential for harm they will not be damaged or that if they do incur harm, they will be made whole in some fashion. An individual using an information system to prepare a tax return for filing is vulnerable in three ways:

- software logic: depending on the complexity of the domain, the user may rely on the accuracy of the final product provided by the system and may not have any means to verify the system output
- system privacy: private and sensitive information entered into and stored in the system or transmitted by the system may be accessible to unauthorised persons
- system security: the user’s system may be compromised by hackers or subject to the introduction of viruses and other malware such as Trojans.

The impact of trust on an individual’s behavioural intentions regarding the use of new technology has been examined in several Taiwanese technology and tax filing papers (Chang et al., 2005b; Fu et al., 2006; Wang, 2003). The authors of these studies mention trust in security and trust in privacy as important factors and label the combination as ‘perceived credibility’ of the system. We believe that system security and privacy are two
interrelated but distinct concepts. We therefore keep trust in security and trust in privacy independent in our model. We include these factors in the model detailed in Figure 2 and propose that they may impact the choice to use tax preparation software.

**Figure 2** System and relationship trust model

In addition to system trust, individuals using information technology in a complex domain environment also must trust the recipient of the information, the ‘associated entity’, and the creator of the software. Trust in the creator of the system and trust in the associated entity are both necessary because both relationships may result in harm to the system user. In the context of this study – individual tax preparation and filing – the user may be harmed because the creator did not apply due diligence when programming the software or does not provide the services promised – such as audit support or system updates. The user may also be harmed if the IRS does not ensure safe transmission and storage of electronic data. While this risk also exist for paper returns, it is reasonable to believe that storing data electronically increases potential risk. Further, taxpayers may be harmed if the IRS makes mistakes when examining and analysing an individual’s tax information. Consequently, our initial model includes two dimensions of relationship trust, trust in the creator and trust in the associated entity. We sought to explore the antecedents to trust in the creator and associated entity. Figure 2 details the relationship between system trust and relationship trust.

A unique and novel aspect of the tax context is the two-step process related to tax preparation and tax filing. We posit that the importance of the different dimensions of trust depends on the step. In the first step, individual taxpayers decide whether to use tax preparation software. Individuals have the choice between preparing their taxes by hand,
using tax preparation software, or hiring a professional tax preparer. Individuals will use the tax preparation software if they believe that the benefits of using the system outweigh the cost. The dimensions of trust that will matter most are trust in the system logic and trust in the creator of the software. In addition, depending on the system setup, individuals will also be concerned with the privacy protection and security built-in the tax software. For example, if the software and/or software updates are obtained through the internet, individuals face the potential of privacy and security risks.

Figure 3  Multi-dimensional trust and the two-step process of tax preparation and e-filing
In the second step, individuals who have used tax preparation software to prepare their tax returns can choose between filing their tax information electronically or via regular mail. Note that electronic filing is not available to individuals who chose to fill out their taxes by hand. Electronic filing implies the transmission of private information through the internet and is, therefore, subject to privacy and security risks. Furthermore, the electronic data is received and stored by the IRS. The trust dimensions that matter most in the second step are, therefore, trust in the privacy protection and trust in the security of the system when transmitting the data electronically. Furthermore, trust in the IRS (the associated entity) is important because security breaches and violation of individual privacy are possible at the information recipient as well. Figure 3 illustrates potential relationships and logic stimulating the different trust dimensions affecting the use of tax preparation software (step 1) and electronic filing (step 2).

4 Methodology

Discovering new antecedents necessitates that researchers explore individual user feelings, impressions and thoughts. Academic inquiry uses different methods of data acquisition including open-ended interviewing, observation and analysis of open-ended items on survey questionnaires (Creswell, 2003). We explored antecedents by posing open-ended questions and allowing users to suggest items that would create, promote or manage the five dimensions of trust (see Appendix). We continued surveying participants and classifying responses until no new suggestions were put forth by respondents.

We collected 17 responses; six respondents were female; eight were male and three individuals chose not to reveal their gender. The ages of the subjects ranged from 32 to 62. Most of the respondents were academic faculty members and/or IT professionals. We analysed the responses from each participant and classified their answers before proceeding to the next response. The classifications emerged as respondents repeated similar antecedents to the open-ended questions. We then developed a typology containing the traditional antecedents technological, institutional, knowledge-based and several novel untested antecedents.

5 Results

Our survey respondents confirm that individuals do relate technological features, personal experience, system reputation, and attest by institutions to the five dimensions of trust. Specifically, technological antecedents relate to individual trust in the system security and privacy; knowledge-based antecedents promote trust in the logic as well as relationship trust, and institutional antecedents are important for all five dimensions of trust. In addition to these established antecedents, our respondents put forth novel and untested precursors that were grouped into the following categories:

- Declarative antecedents – statements, such as the company’s privacy policy or certain promises made by the creator of the software and/or the associated entity. These statements may promote all five dimensions of trust depending on the nature of the statement or promise made.
Reparative antecedents – relate individual user ability to seek legal recourse if they are harmed. Direct reparative antecedents are mean actual legal liability based on statutes or regulations. Certain characteristics that increase the creator’s or the associated entity’s risk – such as their size or the domain in question – can be considered indirect reparative antecedents.

Control antecedents – concerning user ability to individually tailor the system, control the installation of the system, and permit electronic data transmission on a case-by-case basis can be classified as power or control-based antecedents. Individuals trust security, privacy and logic of the system more if they feel they are in control.

System antecedents – certain characteristics of the system such as the cost, perceived consistency and accuracy of the results, and forms of data storage relate to the quality of the IT system. Individuals trust security, privacy, and logic of the system more if they perceive that the system is of higher quality. However, individuals also consider a cost benefit analysis and are willing to take some risks if the convenience of the system provides a high benefit.

Capitulation – finally, we include an item that is not an antecedent to trust, but rather an antecedent to using the system in spite of having no trust. If individuals feel overwhelmed by the complexity of the domain, they are willing to take the risk without having assurances related to the product’s quality. For example, several respondents indicated that they ‘take a chance’ when using tax software because the tax law is too complex for them to understand and the software is convenient.

The results of this exploratory research have implications for academics, IT professionals, and policy makers. Software companies may want to consider including declarative and control-based antecedents in order to create, promote and manage user trust in their system. Policy makers should be aware of the importance of reparative antecedents and may want to introduce regulation that increases individual legal recourse in human-IT system relationships. Our study was conducted in the context of one of the largest e-government initiatives to date, namely electronic tax preparation software and filing. Thus, those interested in the success of other e-government programs, such as politicians and public administrators, may be interested to learn more about the different trust relationships and the many (traditional and new) precursors to trust. Finally, we believe that the survey results also imply some ethical issues related to human-IT interactions. The ‘capitulation antecedent’ implies that in the context of high domain complexity, individuals are willing to take a chance even if the risk of being harmed is relatively high. System creators could abuse this disposition by preying on individual lack of domain knowledge. In the context of tax preparation and e-filing, the fact that individuals generally dislike the task and are afraid of having to deal with the IRS exacerbates the ethical dilemma. For example, several tax preparation products offer ‘audit support.’ Users of the system may believe that this relieves them from legal liability toward the IRS should the tax return contain some errors. This is not the case but seldom highlighted by the system creators.
Table 1  System and associated entity antecedents

<table>
<thead>
<tr>
<th>Technological antecedents: reliance</th>
<th>Reparative antecedents: legal</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Secure socket layer</td>
<td>• Independent arbitration body</td>
</tr>
<tr>
<td>• Encryption</td>
<td>• Legal liability</td>
</tr>
<tr>
<td>• Passwords</td>
<td>• Regulatory fines</td>
</tr>
<tr>
<td>• Authentication</td>
<td>• Financial guarantees</td>
</tr>
<tr>
<td>• Tokens</td>
<td>• Risk (financial or other)</td>
</tr>
<tr>
<td>• Security keys</td>
<td>• Size of company</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Experience antecedents: historical</th>
<th>Power antecedents: control</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Personal experience</td>
<td>• Possibility to customise product</td>
</tr>
<tr>
<td>• Personal familiarity</td>
<td>• Ability to tailor product to meet own needs</td>
</tr>
<tr>
<td>• Use in the past</td>
<td>• Product asks for permission before transmitting data over internet</td>
</tr>
<tr>
<td>• Experience with other products by same creator</td>
<td>• Stand alone use versus network use</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Institutional antecedents: transference</th>
<th>System antecedents: quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Certification standards</td>
<td>• Cost of product</td>
</tr>
<tr>
<td>• Independent institution ratings</td>
<td>• Accuracy of results</td>
</tr>
<tr>
<td>• Expert attests</td>
<td>• Data storage</td>
</tr>
<tr>
<td>• Favourable reviews by agencies</td>
<td>• Consistent results</td>
</tr>
<tr>
<td>• External trustworthiness rules</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recognition antecedents: reputation</th>
<th>Capitulation: surrender</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Name in the business</td>
<td>• Take chance</td>
</tr>
<tr>
<td>• Reputation</td>
<td>• Assume with no backing</td>
</tr>
<tr>
<td>• Attests by others</td>
<td>• Complex – just trust</td>
</tr>
<tr>
<td>• Popularity</td>
<td>• Too hard to learn domain</td>
</tr>
<tr>
<td>• Track record</td>
<td>• Benefit outweighs cost</td>
</tr>
<tr>
<td>• Age of company</td>
<td></td>
</tr>
</tbody>
</table>

| Declarative antecedents: intent       |                                                             |
|---------------------------------------|                                                            |
| • Privacy statement                   |                                                             |
| • Privacy policy                      |                                                             |
| • Promises data will not be shared    |                                                             |
| • Promises data is secure             |                                                             |
| • Testimonials of intent              |                                                             |
6 Conclusions and outlook

In this research, we asked whether trust is multi-dimensional in the electronic tax preparation and filing context and what precursors to trust are needed for individuals to choose electronic tax preparation and filing. We show that because of the complex domain environment and the privacy of the subject matter, a new model of multi-dimensional trust and novel antecedents to trust apply. Thus, this study contributes to the literature in two ways. First, based on an extensive literature review, we developed a model that captures multi-dimensional trust in an environment of complex domain. Second we explored how established and novel antecedents relate to the different dimensions of trust. The intersection of tax and technology acceptance is an important area because of its implications for policy, the tax and IT profession, as well as academic research. The research context of tax preparation is interesting because of

1. the high complexity of the tax law
2. the privacy of the subject matter
3. the omnipresence of the issue
4. the current promotion of tax and technology (e-filing) by IRS
5. the relatively high acceptance of the technology by the general population
6. individual taxpayers' ambivalence or negative attitude toward taxes and the government in general.

Our model illustrates that for the two-step process of individual tax preparation and e-filing five dimensions of trust are important. Specifically, individual use of tax preparation software depends on individual trust in the software logic and in the creator of the software as well as their trust in the software’s ability to keep their tax information private and their computing system secure. Individual use of e-filing depends on their trust in the system’s ability to transmit data without allowing security breaches into the personal machine and to keep the tax information private during and after transmission. E-filing is also affected by individual trust in the recipient of the electronic tax information, the IRS.

Multi-dimensional trust as important determinant of individual choice to use tax preparation software and to e-file is affected by various precursors. We used a qualitative survey methodology to investigate these antecedents and the relationship between antecedents to trust and the five dimensions of trust. The results confirm the traditional technology-based, knowledge-based, and institutional antecedents and reveal four novel items, namely declarative, reparative, power-based, and system quality antecedents. Furthermore, we add capitulation, which is not an antecedent to trust but an antecedent to using the system in spite of having no trust. Specifically, our results indicate that in the context of high domain complexity individuals may take a chance and assume the risk because the domain is too difficult to understand and too hard to learn. We believe that these findings have implications for other situations where the domain is relatively complex and the technology serves as surrogate for the domain expert. We also believe that these situations can lead to ethical dilemmas where software creators are tempted to abuse the fact that users cannot verify the system output. It is important that academics, professionals, and policy makers are aware of these situations.
Our model was developed after reviewing extensive trust literature. We used an open-ended research approach to explore people’s feelings about what creates, develops and manages trust in a complex domain. The relationships in the model have not been empirically tested. Future studies may use survey instruments or archival data and quantitative methodology to test the model in various contexts within and outside the tax domain. This model provides a foundation for future technology acceptance research in complex domains.

Acknowledgements

We would like to acknowledge the anonymous reviewers for providing helpful and constructive comments to improve this paper.

References


Toward multi-dimensional trust


Appendix

This survey is part of a research project related to trust in information technology. We are interested in finding out what people believe builds trust in different information systems, and related entities and organisations. If you have any questions or comments about the survey please do not hesitate to contact us.

Trust in system logic

Trust in system logic is defined as the belief that the software correctly applies specific rules in the correct order to complete the work. For example concerning tax preparation software, a user who trusts the system logic expects the steps and flow of the program to apply the tax rules to the entered data. What do you think causes people to trust system logic?

The following items would help create, promote or manage my ‘trust in system logic.’ Please fill in the box.

Trust in system privacy

Trust in system privacy is defined as the belief that the system keeps information private. For example concerning tax preparation software, a user who trusts the system privacy expects that no personal tax information will be divulged to unauthorised people or systems. What do you think causes people to trust system privacy?

The following items would help create, promote or manage my ‘trust in system privacy.’ Please fill in the box.

Trust in system security

Trust in system security is defined as the belief that the information system will be safe from hacking and the introduction of viruses. For example, a user who trusts the system security expects to use the system without introducing viruses or other unsafe software effects into their machine. What do you think causes people to trust system security?

The following items would help create, promote or manage my ‘trust in system security.’ Please fill in the box.

Trust in the associated entity of the system

Trust in associated entity is defined as the belief that the ‘other entity’ in the relationship is truthful and honest in its dealings, keeps its commitments and is competent and effective in its role. The ‘associated entity’ can be an authority, for example the government, or a peer. The ‘associated entity’ may provide information or receive information through the information technology intermediary. For example, a person using tax preparation software who trusts the ‘associated entity’ believes that the IRS/government is truthful in its dealings with taxpayers and keeps its commitments. What do you think causes people to trust the associated entity of an information system?

The following items would help create, promote or manage my ‘trust in the associated entity.’ Please fill in the box.
Trust in the creator of the system

Trust in the creator of the system is defined as the belief that the ‘creating entity’ in the relationship is truthful and honest in its dealings, keeps its commitments and is competent and effective in its role. For example, a person using tax preparation software who trusts the ‘creator of the system’ believes that the creator is truthful in its dealings with taxpayers and keeps its commitments. Note: the creator of the system may or may not be the same as the associated entity. For example, TurboTax creates tax preparation software which the user acquires to perform tax preparation for the IRS. TurboTax is the creator of the system and the IRS is the associated entity. What do you think causes people to trust the creator of the system?

The following items would help create, promote or manage my ‘trust in the creator of the system.’ Please fill in the box.