Security and Privacy Trust in E-Government: Understanding System and Relationship Trust Antecedents

Alexander J. McLeod Jr.
University of Nevada, Reno
amcleod@unr.edu

Sonja E. Pippin
University of Nevada, Reno
sonjap@unr.edu

Abstract
This research proposes an E-Government security trust model and develops a typology of antecedents in the context of citizen tax software use and e-filing. We propose that tax software use and electronic filing (e-filing) offer a novel and interesting research setting that is relevant to E-Government and security because of (1) the use of software to complete tax returns by a large portion of the citizenry, (2) the necessity of security for transmittal of information during e-filing, (3) the privacy of the subject matter, (4) the current promotion of e-filing by the American tax collection agency (IRS), and (5) individual taxpayer ambivalence or negative attitude toward taxes and the government in general. We suggest that when the information system serves as surrogate for a tax domain expert several antecedents to security and privacy trust are potential determinants of use.

1. Introduction

Trust in information system security and privacy in the E-Government domain is a highly relevant topic. Tax preparation software use and e-filing in the United States represents an interesting and important research setting that is directly related to E-government. In 1998, the Internal Revenue Service Restructuring and Reform Act introduced a goal of 80% e-filing for all federal tax returns by the year 2007. Yet many taxpayers still resist using tax preparation software and e-filing for a variety of reasons, including security and privacy concerns. While the U.S. government has set ambitious goals for electronic tax preparation, the e-file growth rate actually declined from 2005 to 2006 by 23 percent [32]. In 2006, 73 million tax returns, about 54% of all returns, were filed electronically with 20 million being filed from personal home computers. In 2007 the numbers were similar with about 80 million returns, 57% of all returns, filed electronically [16]. The Government Accounting Office recommended to Congress that professional tax preparers be required to file client’s returns electronically in order to increase savings – estimated at $68 million per year if tax software use increased to 90 percent [31]. The IRS continues to modernize but states that at the current level of use, getting more taxpayers to e-file will be difficult. In order to file electronically, tax returns must be prepared using tax preparation software. Thus, individual trust in the security and privacy mechanisms of tax preparation software is critical to increase e-filing. In order to improve technology acceptance in the tax context, understanding the various determinants of acceptance and use is important. The context of individual tax preparation is a unique governmental domain where taxpayers choose between using tax preparation software, filling out their tax forms by hand, or employing a professional preparer. The tax preparation software serves as a surrogate for the professional tax preparer. This situation is different from prior research investigating simpler security and privacy trust relationships. Most individual taxpayers are not tax experts and have limited capabilities to verify system output. Thus, they must trust in the security and privacy protections built into the system by the software producer. Anecdotal evidence from professional tax preparers suggests that taxpayers with especially negative attitudes toward the IRS (or the government in general) do not want to e-file because they think they are “doing the IRS a favor.”

The relationship between the individual taxpayer, the software producer, the tax software, and the tax collection agency affects security and privacy concerns. The interaction of these entities through the tax preparation software requires that individual taxpayers trust the security mechanisms involved in transmission of the tax return, the personal privacy protections built into the system, and the tax domain logic programmed into the software. In addition, individual trust of the taxing authority receiving the tax information becomes important. These contextual E-Government issues make security and privacy trust of interest to information system professionals and tax experts, academics, and policy makers.
The relationships between the individual taxpayer, tax preparation software, IRS and the software producer as suggested in Figure 1 reveal that in the tax return preparation context two forms of trust are relevant. First, individual trust in the tax preparation software must be examined and second, trust in the IRS or associated entity must be considered. This means that research models including simple, unidimensional security trust may be insufficient for complex contexts. We argue that because of the complexity of the tax preparation domain and the two-step adoption process, security and privacy trust must be viewed as multi-dimensional. Therefore, the following research questions are posed in this study:

1. Does multi-dimensional trust affect use of information systems in complex domains?
2. What forms security and privacy trust in environments where several entities act together with an information system?
3. What creates trust in complex environments involving associated entities and multidimensional trust?
4. What promotes trust in affiliated entities using a common information system?

If different forms of trust are needed in complex environments, then differentiating between different precursors to these forms of trust is important. Prior studies have examined the relationship between antecedents and trust in information systems. These antecedents have been categorized into several types including technology-based [4], knowledge or experience based [1], and institutional based [33].

The purpose of this paper is therefore to develop a security trust model that considers different forms of relationship trust and also explores antecedents to security and privacy trust within the context of E-Government and tax preparation software. The remainder of this paper is structured as follows. In the following section we provide the theoretical background. Section three and four introduce the research model and methodology. Section five provides the results which are further discussed in sections six and seven. Section eight concludes.

2. Literature review

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 [4, 10, 12]. The relatively high uncertainty and risk involved with E-Commerce transactions – compared to “traditional” shopping – drives research in this area. We find that most information systems studies conducted to date examine trust as single dimension construct [6, 17, 21, 28]. However, recently several researchers have expanded the concept of trust into a multi-dimensional construct, arguing that the complexity of the information system environments requires a more thorough review of the different aspects of trust. For example, Gefen and Straub [11] synthesize some of the trust dimensions found in prior literature and provide a model that allows for multi-dimensional trust using the 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. Note that While most information system studied examine trust as a single dimension construct [6, 7, 17, 27], Gefen and Straub [11] refer to a multi-dimensional trust construct concerning the relationship rather than trust...
in the information system. Paul and McDaniel [22] 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. Similar to Gefen and Straub [11], trust in the relationship with others and not trust in the system is the focus of the study.

2.1. Multi-dimensional trust

Grabner-Kräuter and Kaluscha [15] differentiate between two forms of trust, interpersonal and impersonal, because in the information systems context human-to-human as well as human-to-artifact 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 relationship trust model shown in Figure 1 suggests that this distinction also applies in the tax context.

Based on the proposed trusted relationships in Figure 1, we introduce a multi-dimensional trust construct measuring individual trust in the information system or “system trust”, and individual trust in the relationship with the other entities or “relationship trust”. Trust in the system is further differentiated into 1) security trust, 2) privacy trust, and 3) system logic trust.

Security trust is defined as the belief that the information system will be safe from hacking and the introduction of viruses or other malware. 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. Users systems compromised by security malware might be used as “zombies” to support email spammers or denial of service attacks.

Privacy trust 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 system privacy mechanisms expects that no personal tax information will be divulged to unauthorized people or systems. User systems with compromised privacy might provide others with social security numbers, credit card numbers or other private information.

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 [4].

Relationship trust concerns individual trust in the creator of the software and any associated entities. 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 individual software companies, and the information recipient is the tax collection agency. This may also be the case in other E-Government domains.

Studies in various academic disciplines also examine the many antecedents to trust, such as the length of the relationship and the satisfaction with the other entity’s performance [18]; the cultural environment [26]; organizational policies [14]; managerial behaviors [2]; expertise, openness, cooperation, tactfulness, timeliness, sincerity, congeniality and integrity [13]; and institutional structures, individual disposition and experience [30]. While antecedents to trust have been examined in most social and life sciences, we focus on the findings from information systems research. Investigations of antecedents of trust in information technology attempt to enhance and improve acceptance and trust in order to reduce transaction costs.

Generally, these antecedents can be categorized as follows: technological antecedents, such as password protection, virus scanning software, and firewalls [4], knowledge or reputational antecedents, such as personal experience, history or referrals by friends with experience [1], and institutional antecedents such as seals of approval and certifications [33]. The results of prior studies are mixed with regard to the importance and effectiveness of some of the antecedents to trust [4]. We are not certain that these classifications adequately describe antecedents of trust in the context of complex domains where the information technology serves as domain expert. The goal of this research is therefore to confirm the “established” antecedents of trust in this particular context and to extend the possible antecedent list to assist in establishing a typology of antecedents. Further, this study examines how additional antecedent constructs impact trust and technology use. The result is a new model of the relationships between trust constructs, several antecedents to trust and individual use of information technology.

3. Research model

The relationship trust model shown in Figure 1 implies several forms of trust, namely trust in the information system or “system trust”, trust in the associated entity, and trust in the creator of the system or “relationship trust”. These constructs correlate with some distinctions made in prior literature [15]. Figure 2 shows the relationship
constructs “system trust” and “relationship trust” and delineates elements related to the E-Government setting involving tax preparation software.

![Diagram of System & Relationship Trust Constructs]

**Figure 2. System & relationship trust constructs**

In order to investigate the elements and effects of these constructs further, we differentiate system trust based on the traditional definition of trust by Mayer et al. [19]. 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. In trusting, users 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: 1) system security - the end user system may be compromised by hackers or subject to the introduction of viruses and other malware such as Trojans, 2) privacy - private and sensitive information entered into and stored in the system or transmitted by the system may be accessible to unauthorized persons, and 3) 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. Figure 2 shows the inclusion of security trust, privacy trust and logic, trust as elements of system trust.

The impact of trust on individual behavioral intention regarding the use of new technology has been examined in several Taiwanese technology and tax filing papers [3, 9, 29]. 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 and therefore keep security trust and privacy trust separate in our 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. These are the two dimensions of relationship trust. Applying the definition of trust from above, 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 the user may be harmed if the IRS does not ensure safe transmission and storage of electronic data. The user may also 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. Further, taxpayers may be harmed if the IRS makes mistakes when examining and analyzing individual tax information.

Consequently, our model consists of two dimensions of relationship trust, trust in the creator and trust in the associated entity, shown in Figure 2.

As outlined above, the question what creates trust has been asked in many academic studies before. We believe that considering the new multi-dimensional trust model, traditional antecedents to trust may not be adequate in explaining individual use in the complex tax preparation context. Thus, besides the development of a new security trust model in the context of E-Government and tax filing, this paper also investigates how traditional and novel antecedents may impact individual multi-dimensional trust. Prior IT research has examined technological, knowledge or reputational, and institutional antecedents [4, 5, 20, 23-25, 33]. We believe that while these antecedents matter in determining taxpayer multi-dimensional trust, additional antecedents are important as well. Understanding what creates and fosters trust is important for academics as well as IT professionals. If the use of technology depends on individual trust in the system and trust in relationships, then creating and managing the different aspects of trust will improve efficiency and effectiveness of technology use. Using the tax preparation and e-filing context, that means individuals may trust the tax software system, the
Table 1 lists the typology that emerged differentiating novel antecedents discovered during the process. We believe that different types of antecedents correlate more or less strongly with the different dimensions of trust. For example, individual trust in system security or privacy may depend more on technological antecedents than knowledge-based antecedents. Providing a typology for the various antecedents will help understand these relationships.

4. Qualitative survey

Discovering new antecedents necessitates that researchers explore individual perception, impression and thoughts. Qualitative inquiry uses different methods of data acquisition including open-ended interviewing, observation and analysis of open-ended items on survey questionnaires [8]. We explored antecedents to system trust and relationship trust by posing open-ended questions and allowing users to suggest items that would create, promote or manage the five dimensions of trust, security trust, privacy trust, logic trust, associated entity trust, and software producer trust. This survey is provided in Appendix A. Respondents were asked to consider each definition and example prior to responding and encouraged to include any feelings, thoughts or impressions concerning the definition, example or question. Following qualitative research guidelines, we continued surveying participants and classifying responses until no new suggestions were put forth by respondents [8].

5. Survey results

A total of 17 respondents participated in the open-ended questionnaire. Six respondents were female; eight were male and three individuals chose not reveal their gender. The ages of the subjects ranged from 32 to 62 years of age. Most of the respondents were academic Accounting and Information Systems faculty members, IT professionals or tax domain experts. Arguably this sample is not representative of the general population. We analyzed 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 construct questions.

When developed a typology containing the traditional definitions of antecedents: technological, institutional, knowledge-based and added several novel antecedents discovered during the process. Table 1 lists the typology that emerged differentiating traditional and new antecedents and their impacts on multi-dimensional trust constructs.

Technological, knowledge-based and institutional antecedents have been examined in prior research. In general, these antecedents were found to cluster into the following groups. Technological antecedents consisted of respondents seeing the use of passwords, encryption, secure socket layers, security keys, firewalls, etc. as necessary for security and privacy trust. We termed these technological antecedents reliance.

Personal familiarity, experience and use in the past were important to the respondents for logic trust, trust in the creator and trust in the associated entity. In prior research, these antecedents were termed experience based. We named this antecedent group historical.

Certifications, standards, seals of approval, expert attests, etc. made by independent accredited or acknowledged institutions or certain authorities have been labeled institutional. Our respondents confirmed that trust in security, trust in privacy, trust in logic, trust in the creator and trust in the associated entity were all preceded by these types of rating elements that transfer responsibility for judgment to others. Thus, one characteristic of these institutional antecedents is transference.

The results of our qualitative survey confirm that individuals do relate reliance, historical and transference features to system and relationship trust constructs. In addition to these “traditional” antecedents, our survey revealed novel antecedents that we grouped into the following categories.

The age of the company, reputation, popularity and other recognition type antecedents made up the next classification. This group of forerunners were reported necessary by our respondents for security trust, logic trust, creator trust and associated entity trust. We classified this group as antecedents of reputation.

Statements concerning a company’s privacy policy or certain promises made by the creator of the software and/or the associated entity comprised this classification. These promises were meant to assure the user of the intent of the creator without legal enforcement. These statements promote security trust, logic trust, producer trust, and associated entity trust. We labeled these dimensions intent.

The next classification of antecedents can be distinguished from declarative antecedents because in addition to a promise by the software creator or the associated entity, respondents also look for some form of legal enforcement. Antecedents related to individual user ability to seek legal recourse or liability if harmed made up this grouping.
Table 1. Antecedent-construct results

<table>
<thead>
<tr>
<th>Traditional Antecedents</th>
<th>Examples</th>
<th>Construct</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technological – Reliance</td>
<td>Passwords, encryption, secure socket layers, security keys, firewalls, etc.</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy</td>
</tr>
<tr>
<td>Experience – Historical</td>
<td>Personal familiarity, experience and use</td>
<td>Logic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Associated Entity</td>
</tr>
<tr>
<td>Institutional - Transference</td>
<td>Certifications, standards, seals of approval, expert attests, etc. made by independent accredited or acknowledged institutions or certain authorities</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Associated Entity</td>
</tr>
<tr>
<td>Novel Antecedents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recognition - Reputation</td>
<td>Age of the company, reputation, popularity and other recognition types</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Associated Entity</td>
</tr>
<tr>
<td>Declarative - Intent</td>
<td>Promises and statements concerning a company’s policies</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Associated Entity</td>
</tr>
<tr>
<td>Reparative Antecedents – Legal</td>
<td>Ability to seek legal recourse or liability if harmed, legal statements</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logic</td>
</tr>
<tr>
<td>Power-based Antecedents - Control</td>
<td>Control over the installation of the system, ability to individually tailor the system, and permit electronic data transmission on a case-by-case basis</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logic</td>
</tr>
<tr>
<td>System-based Antecedents - Quality</td>
<td>Perceived consistency and accuracy of the results, cost, and forms of data storage relate to the quality of the system.</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logic</td>
</tr>
<tr>
<td>Capitulation Antecedents - Surrender</td>
<td>“Just take a chance” because the tax law is too complex, feeling overwhelmed by the complexity of the domain, willing to take the risk of using the software to achieve their goals</td>
<td>No trust</td>
</tr>
</tbody>
</table>

These elements preceded trust in security, trust in privacy, trust in logic and trust in the creator but not the associated entity. We named this classification legal.

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 made up the next group. These antecedents were found to lead to trust in security, trust in privacy and trust in system logic but had no affiliation with trust in the creator or associated entity. That is, they represented system trust only. These antecedents comprise features or mechanisms that allow users to be in control or take power over their systems. Our term for these antecedents is control.

Respondents informed us that certain characteristics of the system such as the perceived consistency and accuracy of the results, cost, and forms of data storage relate to the quality of the system. Individuals trust security, privacy, and logic of the system more if they perceive that the system is of higher quality. These precursors to trust were deemed system related and we therefore termed this classification – quality.

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. Our
respondents reported that if an individual feels overwhelmed by the complexity of the domain, they are willing to take the risk of using the software to achieve their goals. For example, several respondents indicated that they “just take a chance” when using tax software because the tax law is too complex for them to understand. We termed these surrender.

In summary, respondents to this qualitative open-ended survey provided information related to nine antecedent types, namely reliance, historical, transference, reputation, intent, legal, control, quality and surrender classifications. This typology of antecedents to system and relationship trust is shown in Figure 3.

![Figure 3. System and relationship antecedents](image-url)
6. Limitations

The limitations associated with this work are related to the selected methodology and participants. This study relied on a qualitative survey to explore antecedents and will require further study to determine if results are consistent. The number of respondents and their attributes pose limitations that can be addressed in future work.

7. Discussion

These results have implications for academics, IT professionals, and policy makers. Software companies may want to consider including intent and control based antecedents in order to create, promote and manage user trust in the system. Policy makers should be aware of the importance of reparative antecedents and may want to introduce regulation that increases individual legal recourse in E-Government systems.

Finally, we believe that the survey results also imply some ethical issues related to system and relationship trust 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 present. 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 errors. This is not the case but seldom highlighted by the system creators.

8. Conclusion

The intersection of tax and technology acceptance is an important E-Government area because of its implications for policy, information system and tax professionals, as well as academic research. The research context of tax preparation is interesting because of (1) the use of software to complete tax returns by a large portion of the citizenry, (2) the necessity of security for transmittal of information during e-filing, (3) the privacy of the subject matter, (4) the current promotion of e-filing by the American tax collection agency (IRS), and (5) individual taxpayer ambivalence or negative attitude toward taxes and the government in general. 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, we propose a model that captures multi-dimensional trust in an environment of complex domain and second we explore how traditional and novel antecedents relate to multi-dimensional trust.

Our trust 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 an important determinant of individual choice to use tax preparation software and to e-file is affected by various antecedents to trust. We used a qualitative survey methodology to investigate these antecedents and the relationship between antecedents to trust and multi-dimensional trust. The results confirm the traditional technology-based, knowledge-based, and institutional antecedents and reveal several novel items. Our typology distinguishes between recognition, 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. 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 this potential for abuse. Our model was developed using a qualitative research approach. Future studies may use survey instruments and quantitative methodology to test the model in various contexts. Additionally, it would be interesting for future work to examine other complex systems to see if capitulation is an antecedent in other settings.
9. References


Appendix A: Questionnaire

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?

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 unauthorized people or systems. What do you think causes people to trust system privacy?

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?

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?

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?