

Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: An exploratory study of government–citizens online interactions in a turbulent environment[☆]

JinKyu Lee^{a,*}, H. Raghav Rao^b

^a *Management Science and Information Systems, Spears School of Business, Oklahoma State University, OK, USA*

^b *Management Science and Systems, School of Management, University at Buffalo, Buffalo, NY, USA*

Available online 6 June 2006

Abstract

This study examines the relationships between various risks, beliefs, and behavioral intentions that are related to citizens' use of anti-/counter-terrorism e-Government websites. The data was collected through two surveys within a one-year interval — before and after the Iraqi regime was expelled by the US coalition army. The results suggest that perceived privacy risk from an anti/counter-terrorism authority is the major obstacle in citizen-to-government anti/counter-terrorism information flow, while citizens' belief in the authority's domain competence greatly influences citizens' dependence on anti/counter-terrorism website information. Other findings and implications are discussed, and directions for future research are suggested.

© 2006 Elsevier B.V. All rights reserved.

Keywords: e-Government; Perceived risk of terrorism; Trust in national government; Iraq war; Intention to use; Perceived usefulness; Perceived trustworthiness; Structural assurance; System quality; Disposition to trust; Experience with the Internet

1. Introduction

For several years, many government organizations have been trying to transform themselves into more

efficient and effective organizations by adopting new technologies, especially the Internet. At the federal level, e-Government initiatives have developed various web-based public services. For example, FirstGov.gov is a gateway to more than 180 million web pages from federal and state governments, Disasterhelp.gov is an information source for about 15,000 emergency managers, and Grants.gov is a government grant search and application tool for more than \$360 billion in annual grants [13]. State and local level governments also spent more than \$1 billion in 2000 and most of them now provide a portal website for their constituents [14]. However, the increased public concern of terrorism and information security of US citizens is presenting new hurdles to government efforts to leverage efficient technologies. According to a recent poll, 50% of Americans are worried about possible terrorist attacks,

[☆] This paper is based on the authors' preliminary work presented at the ICIS 2003, Seattle, USA. This research has been supported by the National Science Foundation under grant 0548917. The research of the second author has also been supported in part by NSF under grants 0423014, 0420448, 0417095. The usual disclaimers apply. Part of the research of the second author was conducted while he was a Fulbright fellow at the York Centre for International and Security Studies, Canada. The authors would like to thank Prof. Svet Braynov for his help during the initial phase of the research. The authors would like to thank the guest editors for their encouragement in this exercise and the referees for detailed comments that have greatly increased the lucidity of the paper.

* Corresponding author.

E-mail address: jin_kyu_lee1@hotmail.com (J. Lee).

including cyber-attacks on social infrastructure [34]. With the increased role played by the US government in the international community, the threat is unlikely to be dissolved in the near future [46].

Another noticeable trend in the citizen-government interactions is that US citizens' dependency on the Internet for government information and services, especially those related to national emergency, has greatly increased for the last several years [33]. 56% of American Internet users surveyed went online for Iraq war related information, such as how the war was developing over time and how to prepare for possible terrorist attacks. While the war was ongoing, 17% of total American Internet users identified the Internet as the primary information source or communication medium — a big leap from the 3% immediately before the 9/11 incidents [35]. During the same period, ironically, many government agencies had to take down previously available public information from their websites for national security reasons in spite of the increasing demand for online government information. These conflicting pressures from technology utilization, security concerns over the external threat (i.e., terrorism), and government control for public information can create perturbation in the citizens' e-Government acceptance decisions and behavior, which in turn can prevent e-Government initiatives from understanding why some e-Government services are readily accepted while some others fail to attract citizens. What are the risks that citizens are concerned with in the context of Anti-/Counter-Terrorism (ACT hereafter) e-Government service use? When citizens face a high terrorism risk, will they rely on an ACT e-Government website for safety information and provide sensitive information to the website? If not, how can e-Government agencies improve their services and realize the potential benefits of IT? Understanding public perception of risk and interaction with ACT websites are a critical step to effective risk-communication practice [40], yet few researchers have explored factors influencing citizens' use of ACT e-Gov services, and virtually nothing is known about the effect of external threats and counter-measures for the interference of the threats [24].

This study has a two-fold contribution. First, based on user acceptance theories in the MIS field and psychology-based economic theories of decision under uncertainty, we synthesize a model that can explain the role and influence of specific beliefs on citizens' decision to use ACT e-Government websites. Second, it empirically examines the effects of various types of risks and counter-beliefs in the ACT e-Government service context. The types of risks include: (a) possible

terrorist attack, (b) uncertain web-based service channel performance, (c) future behavior of ACT e-Government service providers and the highest government authority in the country, the national government,¹ and (d) information security and privacy risk from the Internet. In relation to these risks, we bring in counter-beliefs that are hypothesized to reduce the perceived levels of risks. The resulting model can take into account the effect of each perceived risk and the counter-effects of the related beliefs, on citizens' intention to use ACT e-Government services.

The invasion in Iraq and its subsequent occupation by the US provided a unique opportunity to study citizens' use of e-Government websites in a risky situation. Because the US government took the leading role in the war, the risk of terrorist attack by the Iraqi regime or other adversaries was significantly increased, and the Department of Homeland Security (DHS) had to raise the national terrorism threat level to High (level orange). We conducted the first questionnaire survey when the war in Iraq was rapidly developing and the alert level was orange. The second survey was conducted exactly a year later, when the alert level was lowered to yellow, despite reports of US casualties on a daily basis.

2. Theoretical background

In this section, we first present the underlying rationale of our dependent variables, and then discuss the theoretical framework and relationships between the concepts included in our analysis.

2.1. Intention to use e-Government services

The motivations of this study (i.e., promoting dependable ACT e-Government services and assuring proper functioning of ACT activities in a public emergency situation) are in line with the concept of information systems success at both user and organizational levels. In this study, we combine both perspectives and propose to use the concept of "intention to use e-Government website" to reflect user satisfaction and approximate achievement of organizational objectives. A government can be understood as either a protector or a controller of its citizens. When it is the protector, its citizens are both consumers of the protection service and sensors (i.e., eyes and ears) of the protector. In contrast, a government as a controller can regulate and punish, if

¹ In the US government, this concept can be understood as the federal level legislative bodies backed by some executive bodies.

necessary, its constituents to uphold institutionalized order [4]. In this case, an individual citizen becomes vulnerable to whatever action is taken by the government. In the e-Government context, citizens' satisfaction with respect to their government as a protector is determined by the quality of protection services provided by e-Government systems. From the government's perspective, its performance as a protector is largely dependent upon its capabilities to gather intelligence and mobilize citizens through e-Government systems. Yet, the controller role of many ACT authorities (e.g., the Federal Bureau of Investigation, police) opens up the possibility that any private information provided to or any behavior suggested by the authorities cannot only be used for public protection but also for control over individuals. Therefore, citizens' willingness to be informed by, follow directions of, and provide information to e-Government reflects the success of ACT e-Government. Based on this viewpoint, we use two intention measures: citizens' *Intention to Depend on Information from an ACT e-Government website (IDI)* and *Intention to Provide private Information to the website (IPI)*. These website level intention measures (as opposed to organizational or specific

function level measures) are more useful than actual usage behavior in this context for two reasons. First, the use of most e-Government websites is voluntary, and actual usage behavior, especially such behavior as providing leads and tips of a terrorist attack, does not occur often. We also assume that current e-Government facilities are still in their primitive forms and do not provide every possible service function that citizens need.

2.2. Theoretical framework

Theories of human behavior provide the general framework of our study (Fig. 1), while we adopt decision theories to specify detailed relationships among various beliefs (i.e., perceived usefulness, trusting beliefs, and perceived risks), attitude, and intentions to use an ACT e-Government website. Included in the theoretical foundation are the Theory of Reasoned Action (TRA) [1] and its extensions in the MIS field [16,28,43], Subjective Expected Utility (SEU) theory [38,39], and Prospect theory [21]. In the following sections, previous studies in the IT acceptance area are briefly introduced and then the relationships between

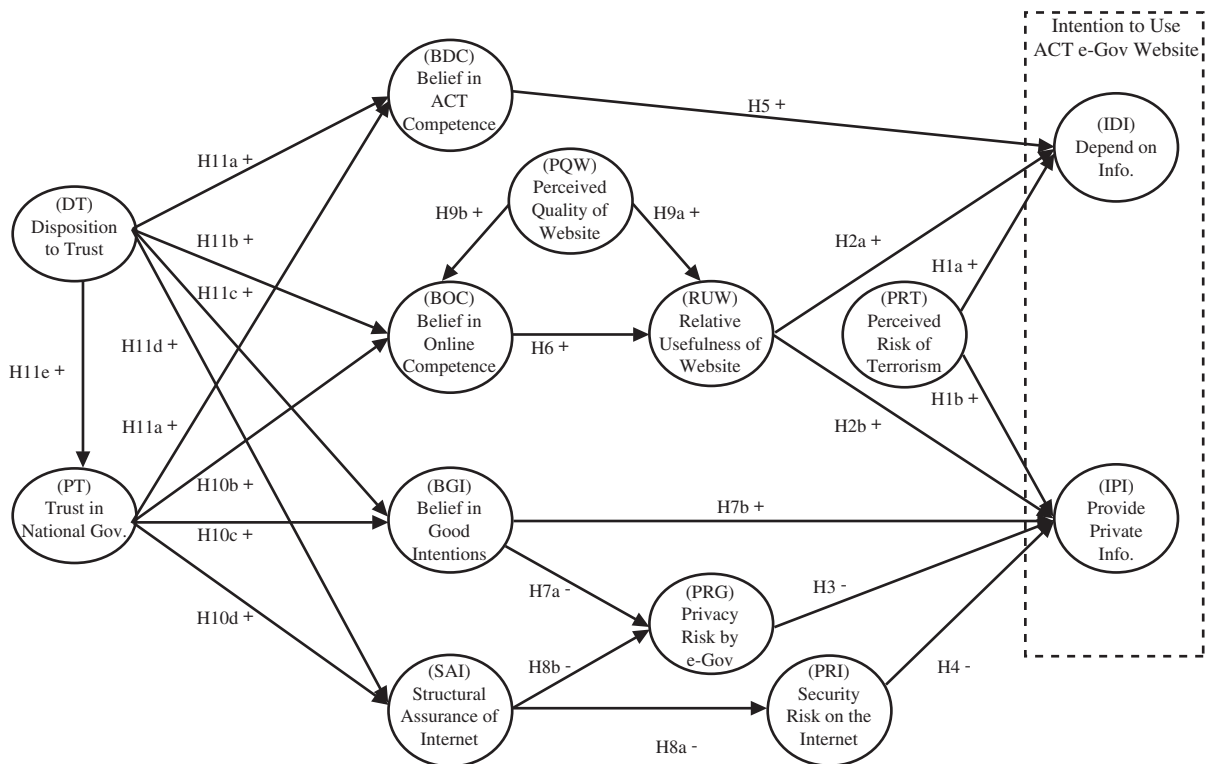


Fig. 1. Hypotheses and structural model of citizens' intentions to use ACT e-Gov websites.

the specific concepts are hypothesized based on decision theories.

2.2.1. Perceived relative usefulness of ACT e-Gov websites

Factors that determine or predict user acceptance of information systems have been one of the most intensively examined topics in MIS studies. The Technology Acceptance Model (TAM) based studies [10] contend that a potential user's acceptance and use of an information system can be best explained by perceived usefulness, perceived ease of use, and a subjective norm. The TAM model was built on the Theory of Reasoned Action (TRA) that views human behavior as a direct function of behavioral intentions and beliefs as determinants of the intentions. In TAM, perceived usefulness is defined as "the degree to which a person believes that using a particular system would enhance his or her job performance" [10]. This explicitly reflects the expected benefits that come directly from system use. The significant effect of perceived usefulness has consistently been found in most empirical studies [43]. Many other IT use studies also reflect expected benefits as a major factor of IT use/usage intention in the form of task support and future value, superior functionality, instrument for extrinsic rewards, or job performance. Similar to the private sector counterparts, citizens' acceptance of an ACT e-Government service will also be affected by the expected benefits of the service system. However, many government services, including ACT services, are offered through multiple channels. Therefore, utility should be discussed in comparison with other types of service delivery channels, rather than as an absolute value. Furthermore, TAM-based models were usually applied to an organizational IT adoption environment where the job that the information system supports was given as a mandatory task and a potential user can only choose either to use or not to use the information system. These assumptions do not apply to networked public information systems such as online shopping sites on the Internet. In the e-commerce system context, the question can be either the choice of a vendor (i.e., website A vs. website B) or the choice of a channel (i.e., online store vs. physical store). In this case, the traditional organizational IT adoption models fall short of applicability to the vendor choice question. Thus, we use the concept *Perceived Relative Usefulness of ACT e-Government Website* to capture potential ACT website users' belief in the expected (dis)advantages over alternative service channels, isolating its effect within the channel choice problem.

2.2.2. Perceived trustworthiness of ACT e-Gov service provider

In order to answer the vendor choice problem, e-commerce acceptance literature adopted the concept of relational trust. A well cited model of organizational trust defines trust as "a willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party," [26, p.712]. According to the model, trust is determined by a trustor's perception on the trustee's trustworthiness (i.e., ability, benevolence, and integrity) and the trustor's propensity to trust, and leads the vulnerable party (trustor) to enter the risky relationship with the trustee [26]. McKnight et al. extended and applied this model to the e-commerce context [28] where the vendor choice problem became a major concern because of the inherent lack of controllability in the Internet environment. In a similar vein, Gefen and his colleagues also suggested that familiarity facilitates online exchange relationships by reducing uncertainty and building trust [15,16]. More recent studies attempted to integrate the organizational IT benefit-based models and e-commerce trust models and provided empirical evidence that both perceived usefulness and trust can have significant impacts on adoption intentions in both private [16] and public sector [24,25] Internet-based information systems.

2.3. Trust, risk, and decision under uncertainty

While an increasing number of e-service studies support the argument that trust is one of the most critical enablers of online relationships [16,20,23], we need to examine more specific concepts with direct relationships in order to provide prescriptive knowledge and practical insight [25]. This is especially important when we need to analyze widely varying government services, including ACT functions, and to provide practical implications for ACT e-Government service practitioners and researchers. Therefore, we decomposed the high-abstract concept of "trust" into three specific beliefs: *Belief in Good Intentions*, *Belief in Domain Competence*, and *Belief in Online Competence*. The first belief involves a trustee's benevolence and integrity, which are closely related to the trustee's likelihood of (non)opportunistic behavior. On the other hand, the latter two beliefs are not associated with the trustee's intentions. Although a trustee who demonstrates high levels of good intentions, domain competence, and online competence may be more trustworthy, there is no logical reason to expect that these attributes co-vary.

Trust is known to be operative only when a risk exists [29]. Risk in traditional economics-based theories is conceptualized as a function (usually the product) of the probability distribution of possible outcomes and the outcomes' subjective values [37], while the term in the literature of psychology-based consumer behavior refers to subjective probability and severity of negative consequences [9]. Although the former assumes that the probability of every possible outcome is known, accurate and objective probability information is rarely available in reality [38,39], resulting in inconsistent levels of perceived risk among individuals. Uncertainty refers to this ambiguity in probability distribution [29]. As a consequence, perceived risk can be influenced by the available information about risk and the decision maker's beliefs in the information source [18], which are often related to familiarity and trusting beliefs [29]. Following the psychology-oriented views, we define *perceived risk* as an *Expectation of Loss*. Also, we treat the information and beliefs that induce trust and familiarity as the determinants of perceived risk.

2.3.1. Perceived risks in ACT e-Government services

Some studies on risk perception identified and categorized different types of perceived risk relevant to the business environments in question (e.g., financial, performance, physical, convenience, delivery, and business relationship risks) [36]. Similarly, categorizing risk types relevant in the ACT e-Government service context can help clarify the relationships between perceived risks, counter-beliefs, and decision under uncertainty. Table 1 summarizes four salient risks in the ACT e-Gov service context: 1) *the risk of terrorist attack*, 2) *the risk of inferior service system or channel*, 3) *the privacy risk caused by the service provider*, and 4) *the information security risk from the Internet environ-*

ment. When citizen behavior is the concern, risks can also be categorized as inherent or handled risk, depending on the level and controllability of the risk [3,12]. Inherent risk resides at the product category level and consumers cannot do much about this risk (e.g., the risk of terrorism). On the other hand, handled risk refers to the risk associated with a particular brand within a product category after a consumer makes a choice (e.g., an ACT website). The last column in Table 1 shows the corresponding level and controllability of the four risk types in the context of ACT e-Government service adoption.

2.4. Determinants of intentions to use an ACT e-Gov website

Subjective expected utility theory argues that people choose the option that offers the highest subjective expected utility among available alternatives [38,39]. The subjective expected utility of an available option ($SEU(X)$) is calculated by summing all the products of utility of every possible outcome state ($u(x(s))$) and the corresponding subjective probability of the outcome state ($p(s)$). The more recently proposed prospect theory takes almost an identical functional form in its prospect (V) calculation, except that it replaces subjective probability p in the $SEU(X)$ function with decision weight (π) [21].

Faced with the risk of terrorism, a citizen can choose to do nothing and take the full risk of terrorism, or choose to use an ACT e-Government website (i.e., depends on the ACT information or provides private information) to reduce the risk. The choice between these alternatives reflects the attitude of the decision maker toward the ACT e-Gov website usage behavior [21]; the attitude that will largely determine our

Table 1
Risks relevant to the ACT e-Gov service context

Risk	Description	Source of Risk	Level/controllability
Risk 1. Terrorist attack	Expected loss from a terrorist attack (i.e., loss of life)	Terrorists	Service category/inherent risk
Risk 2. Inferior service system	Expected loss (e.g., delayed service, out-dated information) from choosing a web-based ACT e-Gov system inferior to an alternative service system or channel (e.g., mail, telephone, in person).	The service provider's online competence	Specific service channel/handled risk
Risk 3. Relational privacy	Expected loss from providing private information to the service provider who may use the information in an unexpected way (e.g., background check, surveillance).	The service provider's benevolence and integrity	Specific ACT authority/handled risk
Risk 4. Environmental information security	Expected loss from using the Internet infrastructure to interact with an ACT service provider (e.g., identity theft, unstable network).	Technological and legal safeguards	Specific service channel/handled risk

behavioral intention variables [1]. The following expressions² represent three available options:

Option A: do nothing and take the full risk of terrorism:

$$SEU(X_A) = \sum p(s_i)u(-x(s_i)) \quad (\text{Expression 1})$$

Option B: depend on an ACT e-Gov website for ACT information:

$$SEU(X_B) = \sum p(s_i)u(-x(s_i)) + \sum p(s_j)u(y(s_j)) \quad (\text{Expression 2})$$

Option C: provide private information to an ACT e-Gov website:

$$SEU(X_C) = \sum p(s_i)u(-x(s_i)) + \sum p(s_j)u(y(s_j)) + \sum p(s_k)u(-z(s_k)), \quad (\text{Expression 3})$$

where $p(s)$ is the subjective probability of an outcome state s to occur, and $u(x(s))$ is the utility of the outcome at state s .

The separate summation groups represent independent subjective expected utilities from different outcome state sets: SEU from a terrorist attack (the 1st block in Expression 1–3), from the choice of the ACT service system (the 2nd block in Expression 2 and 3), and from disclosed private information (the 3rd block in Expression 3). With these specifications, the three blocks reflect Risk 1, Risk 2, and Risk 3 and 4 in Table 1, respectively.

2.4.1. Terrorism risk to usage intentions

As formulated in the expressions above, the *risk of a terrorist attack* influences the attitude toward depending on an ACT e-Gov website for information (i.e., SEU (X_A) over SEU(X_B)) and the attitude toward providing private information to an ACT e-Gov website (i.e., SEU (X_A) over SEU(X_C)). The difference between two resulting SEU(X)s can be considered as an indicator of the strength of the positive/negative attitude toward the dominating/dominated option. For example, let us assume that a terrorist attack has two outcome states, 0 and -100 (i.e., life or death), and the subjective probability of such an attack to occur is 0.05. Also, assume that depending on information in an ACT

website can reduce the probability of the attack to half and that there is no difference between using the ACT e-Gov website and using other systems (e.g., telephone). Then, the subjective expected utilities for the alternative options and the attitude toward the behavioral intention to depend on the ACT website for information can be represented as below:

2.4.1.1. Scenario 1.

$$SEU(X_A) = [0.05*u(-100) + 0.95*u(0)]$$

$$SEU(X_B) = [0.05*0.5*u(-100)] + [0.05*0.5*u(0)] + [0.95*0.5*u(0)] + [0.95*0.5*u(0)]$$

Assuming the utility of an outcome that coincides with the outcome value, for demonstration purpose,

$$SEU(X_A) = -5, SEU(X_B) = -2.5, \text{ and Attitude}(X_{BA}) = SEU(X_B) - SEU(X_A) = 2.5$$

In this example, the higher subjective expected utility of Option B ($SEU(X_B) = -2.5$) will, in general, result in a positive attitude toward Option B (i.e., depend on ACT e-Gov website for information), and the difference between the two subjective expected utilities (i.e., $SEU(X_B) - SEU(X_A) = 2.5$) is an indicator of the level of the positive attitude toward Option B. Now, let us assume that the subjective probability of such a terrorist attack increases to 0.1, with everything else held constant. The subjective expected utilities and the level of the positive attitude toward Option B will change to:

2.4.1.2. Scenario 2.

$$SEU(X_A) = [0.1*u(-100) + 0.9*u(0)] = -10$$

$$SEU(X_B) = [0.1*0.5*u(-100)] + [0.1*0.5*u(0)] + [0.9*0.5*u(0)] + [0.9*0.5*u(0)] = -5$$

$$\text{Attitude}(X_{BA}) = SEU(X_B) - SEU(X_A) = 5$$

This example shows that increase in the risk of terrorism (Risk 1) can increase the positive attitude toward ACT services, *ceteris paribus*. However, this expected utility based prediction is countered by prospect theory, which is a decision theory offered by Kahneman and Tversky [21]. According to prospect theory, individuals faced with a choice under risk go through a two-phase process, the first phase of which transforms the options into a simpler form by applying

² Although both SEU and Prospect theories provide a framework that matches related concepts in the study context, we use the SEU(X) function form to express the alternative options in the ACT e-Gov service context, and the two theories' assumptions where the more important differences exist are not considered in the expressions.

several operations. One effect of such a simplification is the isolation effect. An *isolation effect* occurs when a decision maker ignores components shared by the alternative options [21,41]. Applied to the same Scenario 1 above, an isolation effect will cancel out the probability p^3 of terrorism that applies to both options (i.e., 0.05 and 0.95) and simplify the options to the following forms⁴:

$$\begin{aligned} \text{Prospect}(V_A) &= [\sum \pi p(s_i)v(-x(s_i))] \\ &= \{0.05*[1*v(-100)] + 0.95*[1*v(0)]\} \\ &\rightarrow [v(-100) + v(0)] \end{aligned}$$

$$\begin{aligned} \text{Prospect}(V_B) &= [\sum \pi p(s_i)v(-x(s_i))] + 0 \\ &= \{0.05*[0.5*v(-100) + 0.5*v(0)] \\ &\quad + 0.95*[0.5*v(0) + 0.5*v(0)]\} \\ &\rightarrow [0.5*v(-100) + 1.5*v(0)] \end{aligned}$$

Assuming that an outcome and its utility are identical, for demonstration purpose, $\text{Prospect}(V_A) = -100$, $\text{Prospect}(V_B) = -50$, and $\text{Attitude}(V_{BA}) = \text{Prospect}(V_B) - \text{Prospect}(V_A) = 50$, which will remain unchanged in Scenario 2.

Therefore, prospect theory suggests that the risk of a terrorist attack be irrelevant to the choice between use and non-use of ACT e-Gov websites. H1a and H1b in Fig. 1 examine this contradiction by hypothesizing *positive effects of perceived terrorism risk on the intentions to use ACT websites*.

2.4.2. Perceived relative usefulness of website to usage intentions

In an earlier section, we argued that the concept of perceived usefulness of an ACT e-Gov website should be considered in comparison to those of other service channels provided by the same service provider. The Risk of Inferior Service System (Risk 2 in Table 1) is caused by the ambiguity in the performance of alternative service systems or channels (i.e., website vs. telephone, mail, person-to-person) [8], a.k.a. choice

uncertainty [42] in the marketing field. This risk perception thus involves an individual citizen's 1) evaluation of the subjective expected utility (SEU) of using a web-based service channel and 2) comparison of the SEU with that of non-web service systems or channels available to the individual. To the extent that the individual's SEU of the web-based service is certain and exceeds that of other channels' $p(s_j) u(v(s_j))$, the decision maker will have a stronger positive attitude toward channel choice behavior (i.e., use web-based service), which will in turn increase intentions to use the website for ACT services. This is the rationale behind the *positive effects of the perceived relative usefulness on the two usage intentions* (H2a and H2b in Fig. 1).

According to our categorization of specific beliefs that induce the concept of trust, the only trusting belief, relevant to the evaluation of usefulness perception, will be the belief in the ACT service provider's online competence, and the other two trusting beliefs in our study (i.e., beliefs in ACT competence and good intentions) should have a constant effect across the alternative service channels. In other words, only when an individual believes that an ACT service provider is knowledgeable about and capable of providing quality web-based online services, the individual will predict more favorable outcome states with higher probabilities, in a decision to use a web-based service. This *positive relationship between online competence belief and perceived relative usefulness of an ACT e-Gov website* is represented as H6 in Fig. 1.

2.4.3. Relational privacy risk to usage intentions

Although ACT e-Gov services, as public services, do not involve risks caused by online payment or product delivery, the citizen-to-government information flow can still create risks in using an ACT e-Gov website. This risk can be divided into two types; *relational privacy risk* (Risk 3 in Table 1) and *environmental information security* (Risk 4). The former risk arises from citizens' inability to control the ACT service providers' future opportunistic behavior. As mentioned earlier, any private information passed to an ACT service provider to reduce the terrorism risk can easily be appropriated for a control purpose as well. Furthermore, the voluntary and covert nature of most ACT services can exacerbate this risk. Citizens will not hesitate to provide private information (e.g., annual income, employment, home address) to the Internal Revenue Service (IRS) because any taxpayer is required to do so, and the IRS will already have such information. Also, people will not mind giving their names, home addresses, and contact information to the

³ We predict that individual citizens would focus mainly on the possibility of a terrorist attack, while government and organizations would consider both the probabilities and magnitudes of various possible outcome states of an attack, in which case both theories would predict a positive impact of perceived terrorism risk on the ACT e-Gov service usage intentions.

⁴ For simplicity, every weighted probability $\pi p(s)$ is assumed to be identical to its subjective probability counterpart.

US Postal Service (USPS) because they know when and why USPS needs the information. In contrast, ACT service providers would not usually have an ACT service user's private information, unless the individual drew attention for some reason, and the usage of collected private information would often be unclear. Therefore, providing private information to an ACT service provider greatly increases the vulnerability of the service user by increasing the number of negative possible outcome states and their subjective probabilities (s_k and $p(s_k)$ in Expression 3). Moreover, the increased vulnerability comes without warrant of corresponding reduction in the risk of terrorism. H3 in Fig. 1 represents this *negative effect of perceived privacy risk in a G2C relationship on intention to provide private information*.

Many trust studies have emphasized the importance of trust in terms of its deterrent effects on expected opportunistic behavior of the trustee [16,26,27]. Our concept of belief in good intention consists of benevolence belief and integrity belief that are closely related to opportunism. Because many decisions to exploit citizens' private information against their interests can be made solely at the service provider's disposal, this privacy risk should be largely accounted for by the belief in the ACT service provider's good intention, and neither its ACT domain competence nor online competence should be influential to the decision. We also hypothesize positive direct relationship between the belief in an ACT e-Gov service provider's good intention and citizens' intention to provide private information to the ACT website. Since our conceptualization of belief in good intention is a central factor of relational trust, the widely accepted positive direct relationship between trusting beliefs and behavioral intentions can be validated against our theoretical structure that assume full-mediation of perceived risk. Based on the discussions, we hypothesize that *the belief in an ACT service provider's good intention has a negative effect on the perceived risk of relational privacy* (H7a) and *a positive direct effect on the intention to provide private information to the ACT website* (H7b in Fig. 1).

2.4.4. Internet security risk to usage intentions

Yet another risk related to the bottom-up information flow exists in the Internet environment. *The risk of information security in the Internet Environment* (Risk 4) results from technological flaws and insufficient legal protection in the Internet environment (e.g., threat of hackers and Internet scam). *Information security* can be defined as "*the protection of information and the*

systems and hardware that use, store, and transmit that information" [45, p. 9]. Although all other information systems share some degree of security risk, the Internet environment is particularly vulnerable to information security risk because the environment is not under the control of a single legal jurisdiction or ownership. Regardless of the online service provider's authority or technological competence level, information security cannot be guaranteed in the Internet environment. An example is the recent hoax emails, in which the senders impersonated a government agency (e.g., FBI, FDIC) to falsely accuse the recipients of illegal online activities or violations of Patriot Act in an attempt to distribute an Internet worm or gather private information. This kind of risk is not contingent upon the possibility of opportunistic behavior or technological competence of a particular online entity (e.g., ACT e-Gov service providers), and must be analyzed separately from the relationship specific factors, such as trusting beliefs [26]. Accordingly, we include *information security risk on the Internet* as a separate construct from the previous one (i.e., relational privacy risk) and test its *negative impact on the information flow from citizens to ACT e-Gov websites* (H4 in Fig. 1).

The e-commerce trust model suggests that institution-based trust has both a direct and an indirect effect on trusting intention, through trusting beliefs [28]. Institution-based trust includes two sub-constructs; situational normality that refers to a trustor's perception of the situation where everything seems normal or in the right order, and structural assurance that refers to the beliefs that legal and technological safeguards are in place to protect the trustor. When measured at the Internet infrastructure level, as in [28], the structural assurance concept reflects the situational risk of the Internet environment, while Gefen et al.'s [16] website level manifestation (i.e., existence of 3rd-party seal, 1-800 number, statement of guarantees, and hyper-link with reputable websites) reflects a specific website operator's conformity to situational risk countermeasures and can be considered as a source of relation-specific trusting beliefs. We follow the former view to capture the effects of structural assurance beliefs in the Internet environment in general. This general conceptualization involves factors beyond a particular ACT service provider's attributes (e.g., expertise in online operations, opportunistic behavioral intentions) that can affect both relational privacy risk and extra-relational information security risk on the Internet.

In conjunction with the risks related to providing private information, the structural assurance belief can reduce the relational privacy risk from the ACT service

providers' future behavior (Risk 3) and the information security risk from the Internet environment (Risk 4) [11,28]. According to the results of a large-scale survey [32] on citizens' use of the Internet, on the day of the 9/11 terrorist attack, 4–5 million people used the Internet to contact others because the telephone network was disrupted. Ironically, that was exactly when major Internet news websites (e.g., www.cnn.com, www.msnbc.com) could not be accessed due to their limited bandwidth, and many people without TV or radio (e.g., at work) became anxious to figure out what was really happening. In addition, citizens may not have a clear understanding about the extent to which their government is allowed to delve into their private information (e.g., USA PATRIOT Act). The uncertainty in the Internet environment makes it more difficult to predict what outcome states are possible on the Internet and what their probabilities are. Given the high level of uncertainty, beliefs in the legal and technical structure of the Internet environment can significantly influence the risk perception by reducing the size $-z(s_k)$, the probability $p(s_k)$, and the number k of possible negative outcomes in Expression 3. Thus, we hypothesize that the *structural assurance belief can reduce the information security risk from the Internet environment (H8a) [11,28] and the relational privacy risk from the ACT service provider (H8b).*

2.4.5. ACT domain competence belief to usage intentions

As far as vendor choice is concerned, a decision to depend on an ACT website requires a belief that the ACT e-Gov service provider possesses a certain level of competence in the ACT domain and is capable of reducing the risk of terrorism. Therefore, we hypothesize that an individual's belief in the ACT service provider's domain competence can increase his/her intention to use the ACT service provider's services by increasing the perceived probability of getting useful services ($p(s_i)$ in Expressions 2 and 3). However, it is difficult to argue that the effect of domain competence belief is mediated by the perceived risk of terrorism because using an incompetent ACT service provider's service does not increase the possibility of a terrorist attack. Regarding the intention to provide private information, the belief in domain competence will not affect channel choice (i.e., whether provide private information through a website or another channel to the same ACT authority) because domain competence is an attribute of a service provider and will have the same impact on every alternative channel. Therefore, we hypothesize a *direct positive effect of domain compe-*

tence on the intention to depend on the information (H5 in Fig. 1).

2.5. Effects of trust in national government

Although government organizations have autonomous power and rights to some extent, every government organization is subject to the national (i.e., the highest level) government's control. In such a condition, citizens' trusting beliefs in the national government can be transferred to ACT e-Government service providers through organizational control and cognitive categorization processes [27]. After the 9/11 incidents, the federal government passed several laws that could pose a risk to citizens' rights by controlling information flow among government agencies. For example, the Sensitive But Unclassified (SBU) provision in the Homeland Security Act of 2002 (Title VIII, Subtitle I) enables federal, state and local authorities to share homeland security related information, and allows the President and the Secretary of the Department of Homeland Security to decide on the use and reuse of such information being given to states and localities. The USA PATRIOT Act is another example that increased concern over civil rights, and yet, additional legislations, such as Patriot II (a.k.a. Domestic Security Enhancement Act of 2003) and Intelligence Authorization Act of 2005, are continuing to threaten citizens' privacy and freedom.

In addition to its organizational control, the trustworthiness of national government can influence beliefs in other government organizations by cognitive categorization processes. According to McKnight et al., [27] people tend to trust an unfamiliar entity if the entity is a member of a reputable organization, and vice versa (a.k.a. reputation categorization). Gefen et al. [16] also recognized this cognitive process as an antecedent of trust (i.e., cognition-based trust antecedents). Although most e-Gov service providers are fairly familiar government agencies, where the effect of cognition-based trust is expected to disappear, we argue that the effect exists in the e-Government context. In the e-commerce environment, each online service provider is autonomous and independent entity. Therefore, as an individual experiences an online entity, the entity's disclosed attributes (e.g., trustworthiness) tend to deviate from the industry average. However, in the e-Government context, every online service provider is, in a sense, part of a larger government organization, with the national government at the top of the authority pyramid. Therefore, they will share considerably more attributes (e.g., privacy protection standards,

performance metrics), resulting in convergence around the national government's attributes. In this case, citizens will maintain a relatively static association between beliefs in the national government and those in other government organizations. Hence, we hypothesize that *political trust will have positive effects on the three specific trusting beliefs*. These relationships are presented as H10a–c in Fig. 1.

As the highest legislative and executive body, the national government can also affect perceived structural assurance of the Internet by imposing regulations on the industries. Because structural assurance includes legal safeguards by definition, citizens' beliefs that the national government would protect their online activity by providing appropriate regulatory measures will increase their structural assurance belief. The Children's Online Privacy Protection Act (Coppa), the Gramm–Leach–Bliley Act for the financial industry, and the Health Insurance Portability and Accountability Act (HIPAA) exemplify such influence. We hypothesize a *positive effect of political trust on the structural assurance belief* (H10d in Fig. 1).

2.6. Control variables

The suggested model includes two control variables, *Perceived Quality of a Website* (PQW) and *Disposition to trust* (DT), in order to avoid spurious correlation caused by a common antecedent. *Perceived Quality of a Website* captures the quality of website specific properties such as organization of contents, navigational quality, retrieval speed, and interactivity. As citizens experience the quality, they can revise their previous beliefs in the relative usefulness of the website [22,31]. A high quality system can also provide website users with a signal that the website operator has the competence to carry out online services [16]. McKnight et al. also included a similar concept (i.e., perceived site quality) in their e-commerce trust model as a control variable [28] and hypothesized that perceived site quality can positively influence perceived trustworthiness (i.e., trusting beliefs). Accordingly, we hypothesize that *the perceived quality of a website has positive effects on both, perceived relative usefulness of the website* (H9a) and *the belief in online competence* (H9b).

Disposition to trust (DT) has been suggested to have positive effects on multiple trust factors (i.e., institution-based trust, trusting beliefs, trusting intentions) [15,28]. When the effect exists, not considering the disposition effect will result in spurious correlations between trust in national government, structural assurance belief, and the

trusting beliefs. Therefore, we include disposition to trust in the model where *disposition to trust are hypothesized to affect all the trust related constructs* (H11a–e).

3. Research design and methodology

In order to examine the effects of the various types of risk, this study conducted two questionnaire surveys at two points of time. The first survey was conducted in April 2003 when the battle in Iraq was intense and the Department of Homeland Security issued a high level (level Orange) terrorism alert. The second survey was conducted in April 2004, about 11 months after the US President declared the victory over the Iraqi regime, when the casualty figure was still growing by frequent partisan attacks and insurgency. This repeated survey research was designed to achieve several research goals. Since one of the research objectives is to understand how to secure the stable functioning of e-Government services when the risk of terrorism exists, the survey data should be able to capture the citizens' perception of such a risk. Perceived terrorism risk measured during a peaceful time would not allow the researchers to cover a wide range of possible risk perceptions, which will make relationship detection more difficult. Furthermore, the data gathered in two consecutive years can provide useful insights about the trends in public perceptions and intentions, especially on trust in national government, and provide the research findings with some degree of generalizability.

The survey was conducted in a large northeastern US university located near the US border. For the first survey, three versions of questionnaires were prepared to measure equivalent constructs for three different e-Government websites; the New York State Office of Public Security (NYSOPS), Federal Bureau of Investigation (FBI), and the New York State Department of Motor Vehicles (NYDMV). These websites were selected to represent two levels (i.e., federal and state) and two roles (i.e., ACT and Non-ACT) of e-Government service providers. These questionnaires were randomly distributed to 240 students enrolled in an undergraduate-level management course and yielded 177 responses (73.8%). Extra credits (less than 5 points) were provided to the survey participants, but the participation was voluntary with an option to choose another task for the same number of extra credits. Participating subjects were required to examine the informational content and transaction functions of a specified e-Government website before answering the questionnaire. The same

procedure⁵ was followed during the second survey, which was administered to 219 undergraduate-level students in a management course similar to the one used in the first survey. 137 completed questionnaires were returned (62.6% response rate), and the Department of Homeland Security's terrorism threat advisory level was "Elevated" (level Yellow) during the second survey period. The time window for both surveys was 2 weeks, and there was no dramatic change or significant event in the reported war situation (e.g., capture of high-figure Iraqi official, release of execution scene) during/around the survey periods.

The measurement and structured models were analyzed using PLS Graph, a partial least square based Structural Equation Modeling (SEM) tool. PLS is an appropriate tool for testing relationships in a theory development stage. Since this study applies many theoretical relationships originally developed in the private-sector environment to a new context of e-Government, PLS can provide a better insight for further refinement of our model. In addition to the SEM analysis, some additional analyses were also conducted using SPSS. The detailed procedure is described in the Data Analysis section.

3.1. Sampling

Given that the time interval between the two surveys was about 11 months, and the courses where subjects were recruited were similar, the two sample groups can be considered to share the same demographic and psychological characteristics. This sampling method provided us with a homogeneous group of young and well educated Internet literates. The average age of the respondents was 21.4 years; all of them were, at least, in a bachelor's degree program, and 95% of them had been using the Internet for more than 3 years. McKnight et al. argued that these kinds of student samples can be a good proxy for the e-consumer population who are generally younger and better educated than average consumers [28]. A citizen poll also found that American Internet users under age of 30 or with a college education most frequently used the Internet in relation to Iraq war [35]. Even if this homogeneous sample does not represent the total population of American citizens, it represents one of the most intensive Internet user groups, which enabled us to circumvent compounding effects from

different demographic groups. As this was one of the first studies to examine the effects of terrorism risk and trust in government on citizens' e-Government service use, the focus on a narrow group will provide a clearer picture of the decision pattern and a rigid foothold for future theory extension.

Although studies using student subjects have often been criticized for low external validity [17], there were several reasons we believed that the student sample would not compromise the validity and would indeed be beneficial for this study. Unlike many empirical studies in the field of management, our survey does not require the students to have work experience or to imagine a work place environment. As long as they live in the US and are legitimate e-Government service users, the subjects are a perfectly valid sample. This is a fundamental difference that distinguishes our student sample from other studies that require a hypothetical role-play. Our sample is subject to all the risks considered in this study, while the young age could lower the risk aversion factor, which would make the study more conservative. For these reasons, our student sample represents at least a big portion of potential e-Government website users and has high external validity.

3.2. Measurement items

Many measurement items (Appendix Table A-1) included in the questionnaires directly came from or were adapted from previous research. The two types of e-Government usage intentions, intention to depend on information from the e-Government website (IDI) and the intention to provide personal information to the e-Government website (IPI), were measured by four indicators each. They were originally developed in an e-commerce trust measure study [28] and were modified to reflect the specific context of the websites in question. The perceived relative usefulness of an e-Government website (PUW) used three items, which were developed based on the perceived usefulness and relative advantage measures in the IT acceptance and use literature [10,30]. The measures for the three specific trusting beliefs (BDC, BOC, BGI), the Internet structural assurance belief (SAI), and disposition to trust (DT) were adopted from McKnight et al.'s e-commerce trust measurement model [28] with minor changes in the wording. Trust in national government (PT) was measured by three items originally used to measure political trust in the political science literature. The perceived quality of a website (PQW) is an emergent construct that had five formative indicators. Each item represents heterogeneous website system properties that

⁵ We used only two versions of the questionnaire (FBI and NYDMV) in the second survey as the NYSOPS website had withdrawn a transaction function that was required to be examined in the first survey.

have been identified as important quality factors in the e-commerce and website design literature [22,31].

Three new perceived risk measures were developed for the study because there was no readily available one. The perceived risk of terrorism (PRT) measure originally consisted of four 7-point interval scale items, but one item was dropped⁶ in the measurement model testing. The perceived risk of relational privacy (PRG) measure focuses on privacy risks caused by an ACT e-Gov service provider's deliberate behavior. Therefore, this measure accounts for two types of concerns: opportunistic behavior at the ACT service provider's discretion (e.g., recording personal details for a later, undetermined use, background check to evaluate the credibility of public leads) and conformation to a superior government authority (e.g., order from DHS to NYSOPS, new laws like USA PATRIOT). The measure for perceived risk of environmental information security (PRI) also reflects privacy risk aspects, but excludes any effects of the ACT service provider's intention or future behavior. Instead, it focuses on extra-relationship factors such as hacker attacks and the technological robustness of the Internet infrastructure, which may preclude the web-based ACT service channel from being utilized for sensitive information transmission. The PRG and PRI measures have 3-items each, all 7-point scale. Both measures achieved acceptable reliability and construct validity without dropping any item. The standardized weights and loadings of these newly developed measures are shown in the Appendix Table A-1. The results from a reliability and validity test are presented in the next section.

4. Data analysis

After data cleaning,⁷ the resulting 269 cases (Table 2) were first examined for sample group characteristics. In order to provide meaningful information about citizens' threat perception and e-Government usage intentions, group characteristics of the two survey samples should be identical and the only differences between the

⁶ The standardized weight and loading were 0.1523 and 0.2633 respectively. The composite reliability and average variance extracted (AVE) value for the construct were 0.734 and 0.434 before the item was dropped.

⁷ Cases with extremely low variance or logically inconsistent answers to reversed-pair items were dropped from the first survey data. The second survey questionnaire included two sincerity tester items that asked not to answer the items, and respondents who answered any of those tester items were excluded. Obvious patterned-answers were also manually filtered out from the both datasets.

Table 2
Sub-sample size per year and site

	NYSOPS	FBI	NYDMV	Total
2003	54	50	54	158
2004	–	53	58	111
Total	54	103	112	269

datasets should be the duration that the subjects perceived the abnormal event (i.e., the war between the US and Iraq) and the consequent perceptions of terrorism risk and trust in national government. Independent *t*-tests showed that the two groups share the same demographic characteristics in terms of the average length of US residency, Internet use, computer skills, and web skills. Although the differences in the average age and educational level were statistically significant, the cohort group sampling could limit the difference within a one-year gap.

The collected data were divided by the role, and only the ACT data (i.e., NYSOPS and FBI; $n=157$) were used in the structural model testing, while ACT and Non-ACT data were combined in descriptive/comparative analyses ($n=269$). The measurement model was tested using PLS. In the reliability and validity testing stage, two items (refer to Appendix Table A-1) were dropped due to their low face/convergent validity. After the modification in the measurement model, 3 out of our 41 (7 %) reflective indicators' standardized loading were below the desirable level of 0.707 [2,5]. Those three are IDI3 (0.678), PT3 (0.691), and DT4 (0.530). Regarding the IDI measure, it seems that the two reverse worded items (IDI2 and IDI 4) caused a noise and not IDI3. The problematic measurement item for political trust (PT3) is also a reverse worded item. The low loading of DT4 is understandable because it reflects a trusting stance, while the other items (DT1-3) in the construct reflect beliefs within a disposition to trust [28]. As the cutoff level sometimes goes down to 0.5 for a newly developed scale or an application across disciplines [6], we decided to retain the 3 items. Composite reliabilities for all constructs were well over the acceptable level of 0.7, and thus good convergent validity was demonstrated [19]. Discriminant validity was tested by the average variance extracted (AVE) and cross-loadings. Every construct's square root of AVE score was higher than its correlations with other constructs (Table 3). The correlations between construct scores and standardized reflective indicator values also showed that there was no significant cross-loading.⁸

⁸ Available from the authors upon request.

Table 3
Inter-construct correlation and AVE values (AVE in diagonal, NYSOPS and FBI, $n=157$)

	IDI	IPI	PRT	PUW	PRG	PRI	BDC	BOC	BGI	SAI	PQW	PT	DT
IDI	0.568												
IPI	0.140	0.731											
PRT	0.237	0.155	0.570										
PUW	0.358	0.283	0.093	0.606									
PRG	-0.082	-0.466	-0.024	-0.112	0.699								
PRI	-0.078	-0.354	-0.012	0.024	0.675	0.617							
BDC	0.652	0.042	0.230	0.203	-0.048	-0.088	0.807						
BOC	0.545	0.154	0.291	0.364	-0.140	-0.046	0.728	0.844					
BGI	0.465	0.300	0.224	0.309	-0.198	-0.182	0.639	0.646	0.610				
SAI	0.003	0.219	0.012	0.245	-0.169	-0.177	0.158	0.178	0.254	0.771			
PQW	0.474	-0.045	0.031	0.443	0.026	-0.012	0.506	0.525	0.384	0.198	N/A		
PT	-0.087	0.190	-0.178	0.002	-0.113	-0.185	0.098	0.100	0.251	0.294	0.105	0.535	
DT	0.176	-0.018	-0.110	0.092	0.070	-0.006	0.309	0.243	0.287	0.309	0.254	0.250	0.548

N/A: emergent construct with formative indicators.

With the acceptable levels of reliability and validity, we tested the time difference in the exogenous variables (i.e., PRT, PT, DT). For each of the constructs, its indicator variables were averaged to calculate the exogenous variable values, which were then analyzed using the independent t -test function in SPSS. We expected that perceived risk of terrorism (PRT) decreased during the 1 year interval, while all the other exogenous variables remained unchanged. However, the test results show that the average levels of perceived risk of terrorism were statistically identical. Instead, the average level of trust in the national government (PT) significantly decreased during the period (Table 4).

This phenomenon may be explained by the continued conflict between the US troops and insurgents in Iraq. Although President Bush declared the end of major combat on May 1, 2003, with 138 American deaths, the casualty figure continued to increase, exceeding 1000 on Sep. 8, 2004. In addition, there were several perceivable terrorism threats between President Bush's declaration and the second survey period (e.g., the roll back of DHS' terrorism threat level to "high" in Dec. 2003, followed by international flight cancellations and delays caused by terrorism intelligence). Therefore, we can safely assume that the

Table 4
Mean difference in exogenous variables

	2003	2004	Mean difference	t stat. (2-tailed)
PRT	4.134	4.078	0.056	0.374
PT	3.847	3.459	0.388	2.850***
DT	4.632	4.634	-0.002	-0.014

* $p < .05$, ** $p < .01$, *** $p < .005$.

extended period of the external threat hampered the decrease of perceived risk and trust in the US federal government. As mentioned above, the structured model was tested with the ACT data (i.e., NYSOPS and FBI; $n=157$) only. The results from the main analysis are presented in the next section.

5. Results

The graphical results of structural model analyses are presented in Fig. 2. The results show that some relationships found in the private-sector IT/e-commerce acceptance studies also hold in an e-Government context, but some others do not. More than 50% of the variance in the first final dependent variables, intention to depend on information (IDI) is explained by three variables, domain competence (BDC), relative usefulness (PUW), and risk of terrorism (PRT). Among these, BDC has the strongest effect ($\beta = .585$, $p < .01$), yet the effect of PUW is also significant and substantive ($\beta = .243$, $p < .01$). Interestingly, the positive effects of PRT on both dependent variables were not significant ($\beta = .096$, n/s for both paths), thus supporting the isolation effect suggested by prospect theory. Regarding the second dependent variable, the intention to provide private information (IPI), relational privacy risk (PRG) is the strongest determinant with a negative effect ($\beta = -.319$, $p < .01$). Relative usefulness (PUW) also has a significant positive effect ($\beta = .193$, $p < .05$) for this dependent variable. The negative effect of environmental risk of the Internet (PRI) and the positive direct effect of belief in good intention (BGI) are noticeable, but not significant. These antecedents explain about 32% of the variance in IPI.

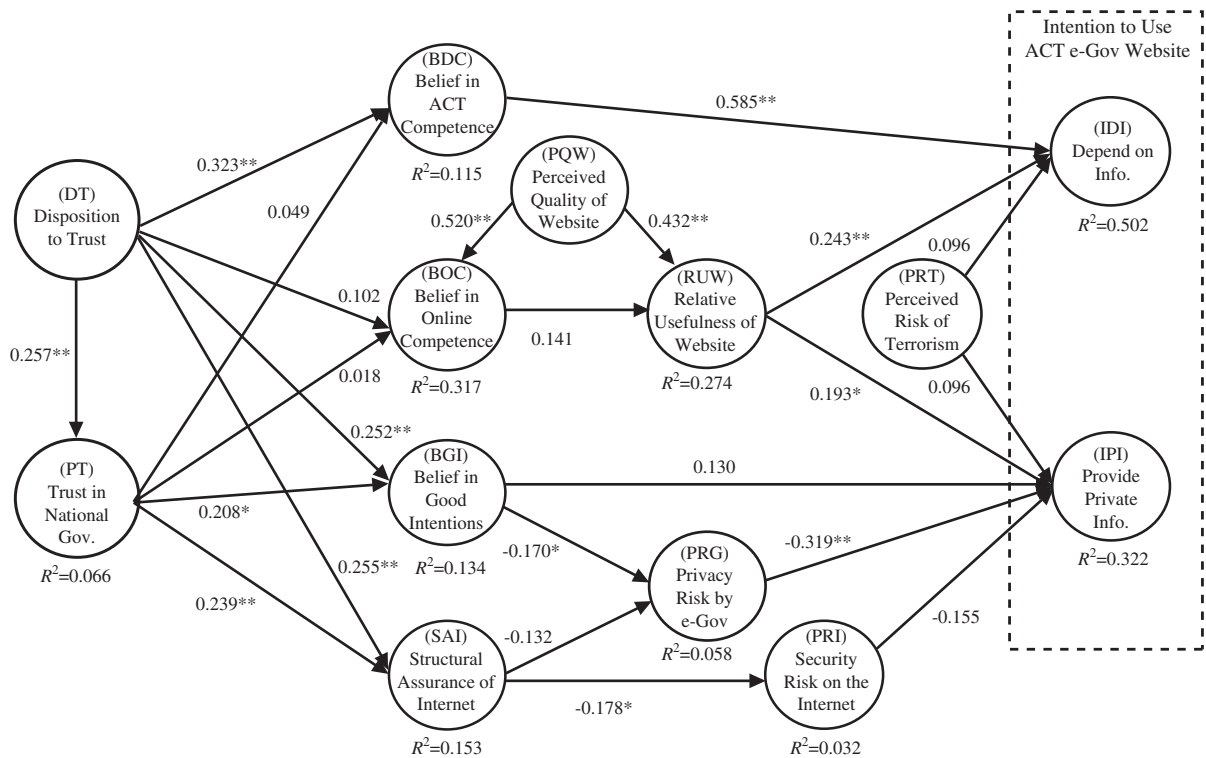


Fig. 2. Hypotheses and structural model of citizens' intentions to use ACT e-Gov websites (NYSOPS and FBI).

Online competence belief (BOC) seems to influence relative usefulness (PUW) in a positive way. However, BOC and PUW perceptions are affected by the same

cognitive stimuli, the perceived quality of website (PQW). PQW accounts for 27% and 32% of the variances in PUW and BOC, respectively. As

Table 5
Summary of hypotheses testing

Hypotheses	Description	Result
H1a. PRT → IDI (+)	Perceived terrorism risk → intention to depend on ACT e-Gov Info.	Reject SEU
H1b. PRT → IPI (+)	Perceived terrorism risk → intention to provide private info to ACT e-Gov	Reject SEU
H2a. PUW → IDI (+)	Perceived relative utility of website → intention to depend on ACT e-Gov Info.	Supported
H2b. PUW → IPI (+)	Perceived relative utility of website → intention to provide private info to ACT e-Gov	Supported
H3. PRG → IPI (-)	Perceived privacy risk from ACT e-Gov → intention to provide private info to ACT e-Gov	Supported
H4. PRI → IPI (-)	Perceived infosec risk from the Internet Env. → intention to provide private info to ACT e-Gov	Not supported
H5. BDC → IDI (+)	Belief in ACT authority's domain competence → intention to depend on ACT e-Gov Info.	Supported
H6. BOC → PUW (+)	Belief in ACT authority's online competence → perceived relative utility of website	Not supported
H7a. BGI → PRG (-)	Belief in ACT authority's good intention → Perceived privacy risk from ACT e-Gov	Supported
H7b. BGI → IPI (+)	Belief in ACT authority's good intention → intention to provide private info to ACT e-Gov	Not supported
H8a. SAI → PRI (-)	Belief in structural assurance of the Internet → perceived infosec risk from the Internet Env.	Supported
H8b. SAI → PRG (-)	Belief in structural assurance of the Internet → perceived privacy risk from ACT e-Gov	Not supported
H9a. PQW → PUW (+)	Perceived quality of website → Perceived relative utility of website	Supported
H9b. PQW → BOC (+)	Trust in the national government → belief in ACT authority's online competence	Supported
H10a. PT → BDC (+)	Trust in the national government → belief in ACT authority's domain competence	Not supported
H10b. PT → BOC (+)	Trust in the national government → belief in ACT authority's online competence	Not supported
H10c. PT → BGI (+)	Trust in the national government → belief in ACT authority's good intention	Supported
H10d. PT → SAI (+)	Trust in the national government → belief in structural assurance of the Internet	Supported
H11a. DT → BDC (+)	Disposition to trust → belief in ACT authority's domain competence	Supported
H11b. DT → BOC (+)	Disposition to trust → belief in ACT authority's online competence	Not supported
H11c. DT → BGI (+)	Disposition to trust → belief in ACT authority's good intention	Not supported
H11d. DT → SAI (+)	Disposition to trust → belief in structural assurance of the Internet	Supported
H11e. DT → PT (+)	Disposition to trust → trust in the national government	Supported

hypothesized, BGI has a significant negative effect on relational privacy risk (PRG) ($\beta = -.170, p < .05$), and the structural assurance of the Internet (SAI) on the environmental risk of the Internet (PRI) ($\beta = .178, p < .05$). However, the negative effect of SAI on PRG is not significant.

In terms of the antecedents of the trusting beliefs in ACT e-Gov service providers, trust in the national government (PT), or its political directions, significantly influences belief in good intention (BGI) ($\beta = .208, p < .05$), but not the others. The disposition to trust (DT) has strong positive effects on domain competence (BDC) ($\beta = .323, p < .01$) and the belief in good intention (BGI) ($\beta = .252, p < .05$) directly, as well as indirectly through the strong positive effect on trust in the national government (PT) ($\beta = .257, p < .01$). Also, both trust in the national government (PT) and disposition to trust (DT) have strong positive influences ($\beta = .239, p < .01$; $\beta = .255, p < .01$) on structural assurance of the Internet (SAI). Table 5 summarizes the results of hypotheses testing.

6. Conclusion and discussion

This study synthesized a model of ACT e-Gov service use, by integrating various IS acceptance theories previously developed in the private sector environment. The model was then applied in an e-Government context to examine the effects of various risk and trusting beliefs on citizens' ACT e-Government service usage intentions. This approach extends previous research by identifying the risks involved in ACT website usage behaviors and testing the counter-effects of trust on the risks, based on theories of decision under uncertainty. In doing so, we decomposed the trust construct, which was often measured as a single abstract belief, into three specific trusting beliefs: *beliefs in an ACT service provider's good intention, competence in the functional domain, and competence in online services*. Our approach to measure specific beliefs about specific attributes of an ACT service provider enables a precise examination of the antecedents and consequence of the beliefs. The study also tested effects of two trust antecedents, disposition to trust and political trust.

The results are interesting. The results suggest that *the perceived risk of a terrorist attack does not increase the citizens' intention to use an e-Government website* significantly. This finding can be explained by the isolation effect and the emphasis on the probability aspect of terrorism risk. Prospect

theory differs from expected utility-based theories in its assumption that decision makers tend to simplify available options at an early stage of decision making process (a.k.a. editing phase), such that components shared by all available options (i.e., online vs. off-line) are canceled out [21]. Another necessary condition to make this no-effect relationship possible is that citizens focus on the probability of a terrorist attack, and not on the size of loss. This is intuitive because the ultimate result of a terrorist attack is the death of an individual — “I will be 1/3 dead with probability of 0.5” does not make sense. However, *this assumption may not hold for risk management personnel in organizational decision cases where the risk should be measured at an aggregated level (e.g., national level casualties in a realized attack) and partial reduction (e.g., reduced number of deaths or social impacts) has an important value*. This exploratory study provides a theoretical foundation and empirical evidence for this issue. However, this relationship and the assumptions should be further examined with a more focused and robust research design.

For ACT e-Gov service providers, this study offers some prescriptive knowledge. They cannot expect that “citizens will use our website if they perceive a risk of terrorism.” Citizens will not depend on ACT website information, unless the information provider has demonstrated a high level of competence in protecting citizens from a terrorist attack and the web-based service has an advantage over an alternative service source (e.g., NGO or private sector organizations) or channel (e.g., TV or mobile network). If an ACT e-Government service provider needs information input from the public, it also needs to guarantee that it will not misappropriate gathered private information. Citizens' perception of privacy risk from ACT e-Gov service provider (PRG) has a strong negative impact on the intention (IPI), and technological/legal safeguards (SAI) may not reduce this risk effectively.

In conjunction with privacy risk, *finding major determinants of the risk perception (PRG) and the belief in the good intention (BGI)* is a pressing issue for future research. In this study, it was evident that belief in the good intention of an ACT service provider is mediated by relational privacy risk and does not have a significant direct effect on usage intention, favoring our risk-centric model over previous trust-centric models for ACT e-Government studies. Nevertheless, the statistically significant effect of the good intention belief explains less than 6% of

the variance in the relational privacy risk. Regarding determinants of the specific trusting beliefs, the trust in the national government can flow into the belief in good intention of ACT service providers and the belief in structural assurance of the Internet environment, but does not influence competence beliefs (neither domain nor online). Together with the disposition to trust, the trust in national government (PT) accounts for only 15% or less of the variances in the relational trusting beliefs. Considering the important role in ACT e-Gov services, it is very critical to find major determinants of the perceived relational privacy risk and the counter-beliefs.

This study established theoretical relationships between risks in the ACT e-Gov service context and their counter-beliefs. The relationship structure, which is based on decision theories, offers a transparent view of the behavioral belief and attitude formation in the behavioral theory. However, this paper does not talk clearly about the effects of social and control factors [1] in behavioral theories. For example, even though more than 30% of the online competence belief (BOC) was explained by the perceptions from website quality (PQW), other sources of information (e.g., Information about the federal level government agencies' low competence in information security [44] from social/Internet/mass-media networks) may also have the same effect. *Exploring those factors outside of the rational decision making process will be very beneficial to ACT e-Gov service providers and MIS researchers alike.* One way to address this gap would be a country level comparison or a cultural study. Since our model was tested only with American citizens, studying people in a different context (e.g., UK, Spain, Australia, as well as Middle eastern countries) will clarify the boundary condition of this model and may suggest additional or different sets of influential factors.

In terms of the research design, there are several issues that this study could not clearly address. First, due to the website change during the study period, we could not include the NYSOPS website in the 2nd survey. Although the sample size is still much larger than the minimum requirement of the statistical analysis tool [7], data from a single website in the 2nd survey might reduce the generalizability or statistical power of the results. The homogeneous sample groups would represent a large portion of prospective e-services users, but this fact also limits the generalizability of the results. As online interaction gains wider acceptance throughout the popula-

tion, more casual computer users should be included in a future study. Our repeated surveys with one-year interval allowed us additional confidence that the identified relationships would be generalizable across time. However, the long survey interval created challenges in terms of the internal validity of the model and the measurement validity. That is, any event during the study period could influence the survey participants' intentions to use an ACT website as well as its determinants. Although such environmental stimuli were what enabled us to include a wider range of responses (esp. PRT), some other factors not included in our model could also affect the dependent variables in the model. Also, such changes required us to modify wordings of some measurement items (PRTx in Appendix Table A-1), posing a potential threat to the comparability of the measurement instruments. In order to overcome these limitations, one may adopt an experimental design or longitudinal survey research design in the future study. We expect that our findings, limitations, and future research directions discussed here can provide valuable insights and a rigid foothold for the homeland security and emergency management research community.

Appendix A

Table A-1
Measurement items (FBI version: *WebSite X*=www.fbi.gov)

<i>Intention to use ACT e-Gov services</i>	
IDI1. When a public security concern arises, I would feel comfortable depending on the information provided by WebSite X.	
IDI2. I cannot depend on information from WebSite X for critical public security problems.*	
IDI3. Faced with a difficult public security problem that required me to behave in a certain way, I would follow the directions of WebSite X.	
IDI4. If I have a public security concern in the future, I will not seek information at WebSite X.*	
IPI1. I would be willing to provide my personal information like my name, address, and phone number on WebSite X if required to use its online services.	
IPI2. I will provide my social security number on WebSite X if needed to use its online services.	
IPI3. I would be willing to share the specifics of my situation like my job, interests, and family information with WebSite X if required to use its online services.	
IPI4. I would be willing to provide my credit card information on WebSite X if I want to pay for any valuable services on it.**	
<i>Perceived risk of terrorism</i> [2003 version 2004 version]	Std. loading (weight)
PRT1. The [war US stationary troops] in Iraq has created an emergency in the US.	0.769 (0.452)

Table A-1 (continued)

	Std. loading (weight)
<i>Perceived risk of terrorism</i> [2003 version 2004 version]	
PRT2. [This war Involvement of the US government in post-war development of Iraq] will require me to be constantly vigilant for terrorist acts in the US.	0.714 (0.420)
PRT3. The [war Involvement of US] in Iraq development has decreased the quality of life in the US.***	–
PRT4. The [war tension between the US and Iraq] makes me concerned for my safety in the US.	0.780 (0.459)
<i>Perceived relative usefulness of website</i>	
PUW1. Using WebSite X can save my time, compared to dealing with real people for the same service.	
PUW2. Using WebSite X can improve the service quality that I will receive, compare to dealing with real people for the same service.	
PUW3. Using WebSite X can be more effective than dealing with real people for the same service.	
<i>Perceived risk of relational privacy</i>	
PRG1. My personal information given to WebSite X may be shared with other government agents to whom I do not want to provide the information.	0.815 (0.390)
PRG2. WebSite X may allow another party access to my personal information without my consent.	0.821 (0.392)
PRG3. My personal information may be used in an unintended way by WebSite X.	0.871 (0.417)
<i>Perceived risk of environmental information security</i>	
PRI1. Someone can snatch my personal information while I'm sending the information to WebSite X.	0.711 (0.387)
PRI2. Hackers may be able to intrude WebSite X and steal my personal information stored in WebSite X.	0.862 (0.468)
PRI3. WebSite X is subject to online terrorist attack.	0.776 (0.422)
<i>Belief in domain (ACT) competence of e-Gov service provider</i>	
BDC1. WebSite X is competent and effective in providing public security services.	
BDC2. WebSite X is very knowledgeable about public security.	
BDC3. WebSite X is capable and proficient in public security service.	
<i>Belief in online competence of e-Gov service provider</i>	
BOC1. WebSite X is very knowledgeable about how to provide services on the Internet.	
BOC2. WebSite X is capable and proficient in online service.	
BOC3. WebSite X is competent and effective in providing services on the Internet.	
<i>Belief in good intention of e-Gov service provider</i>	
BGI1. I believe that WebSite X would act in my best interest.	
BGI2. If I required any help, WebSite X would do its best to help me.	

Table A-1 (continued)

<i>Belief in good intention of e-Gov service provider</i>	
BGI3. WebSite X (and its operator) is interested in my well-being, not just its own.	
BGI4. WebSite X is truthful in its dealings with me.	
BGI5. I would characterize WebSite X as honest.	
BGI6. WebSite X would keep its commitments.	
<i>Belief in structural assurance of the Internet environment</i>	
SAI1. The Internet has enough safeguards to make me feel comfortable using it to transact sensitive information.	
SAI2. I feel assured that legal and technological structures adequately protect me from problems on the Internet even in an emergency.	
SAI3. I feel confident that encryption and other technological advances on the Internet make it safe for me to do business there.	
<i>Perceived quality of e-Gov website[†]</i>	
PQW1. WebSite X is effectively organized.	
PQW2. WebSite X provides significant user interaction.	
PQW3. In WebSite X, the speed of information display was too slow*.	
PQW4. WebSite X provides feedback mechanisms.	
PQW5. WebSite X provides useful information.	
<i>Trust in national (federal) government</i>	
PT1. Most politicians in this country can be trusted to do what they think is best for the country.	
PT2. I usually have confidence that the US government will do what is right.	
PT3. No matter what people usually think, only a few people will run this country always.*	
<i>Disposition to trust</i>	
DT1. In general, people really do care about the well being of others.	
DT2. In general, most folks keep their promises.	
DT3. Large majority of professional people are competent in their area of expertise	
DT4. I usually trust people until they give me a reason not to trust them.	
*Reverse-worded item. **Dropped item for low face validity. ***Dropped item for low reliability. [†] Emergent construct with formative indicators.	

References

- [1] I. Ajzen, The theory of planned behavior, *Organizational Behavior and Human Decision Processes* 50 (2) (1991).
- [2] D. Barclay, R. Thompson, C. Higgins, The partial least squares (PLS) approach to causal modeling: personal computer adoption and use in illustration, *Technology Studies* 2 (2) (1995).
- [3] J.R. Bettman, Perceived risk and its components: a model and empirical test, *Journal of Marketing Research* 10 (1973).
- [4] J.O. Bolletton, The customer-centric digital department: e-Service in government, *e-Service: New Directions in Theory and Practice*, M. E. Sharpe, Inc., New York, 2002.
- [5] W.W. Chin, Issues and Opinion on Structural Equation Modeling, *MIS Quarterly* 22 (March 1998).
- [6] W.W. Chin, The partial least squares approach for structural equation modeling, *Modern Methods for Business Research*, Lawrence Erlbaum Associates, London, 1998.

- [7] W.W. Chin, P.R. Newsted, Structural equation modeling analysis with small sample using partial least squares, *Statistical Strategies for Small Sample Research*, Sage Publications, 1999.
- [8] D.F. Cox, S.V. Rich, Perceived risk and consumer decision making — the case of telephone shopping, *Journal of Market Research* 1 (32–40) (1964).
- [9] S.M. Cunningham, *The major dimensions of perceived risk, Risk Taking and Information Handling in Consumer Behavior*, Graduate School of Business Administration, Harvard University Press, Boston, MA, 1967.
- [10] F.D. Davis, Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly* 13 (3) (1989).
- [11] P.M. Doney, J.P. Cannon, An examination of the nature of trust in buyer–seller relationships, *Journal of Marketing* 61 (2) (1997).
- [12] G.R. Dowling, R. Staelin, A model of perceived risk and intended risk-handling activity, *The Journal of Consumer Research* 12 (1) (1994).
- [13] e-Gov, e-Gov and IT accomplishments, <http://www.whitehouse.gov> 2003 (2003).
- [14] D.B. Gant, J.P. Gant, C.L. Johnson, State web portals: delivering and financing e-Service, *The PricewaterhouseCoopers Endowment for The Business of Government*, 2002.
- [15] D. Gefen, E-commerce: the role of familiarity and trust, *Omega* 28 (6) (2000).
- [16] D. Gefen, E. Karahanna, D. Straub, Trust and TAM in online shopping: an integrated model, *MIS Quarterly* 27 (1) (2003).
- [17] M.E. Gordon, L.A. Slade, N. Schmitt, The 'Science of the Sophomore' revisited: from conjecture to empiricism, *Academy of Management Review* 11 (1) (1986).
- [18] A.D. Gurmankin, J. Baron, K. Armstrong, Intended message versus message received in hypothetical physician risk communications: exploring the gap, *Risk Analysis* 24 (5) (2004).
- [19] J.F. Hair Jr., R.E. Anderson, R.L. Tatham, W.C. Black, *Multivariate Data Analysis with Readings*, 4th ed., Prentice Hall, Englewood Cliffs, NJ, 1995.
- [20] S.L. Jarvenpaa, N. Tractinsky, M. Vitale, Consumer trust in an Internet store, *Information Technology and Management* (1) (2000).
- [21] D. Kahneman, A. Tversky, Prospect theory: an analysis of decision under risk, *Econometrica* 47 (2) (1979).
- [22] J. Kim, L. Jung, K. Han, M. Lee, Businesses as buildings: metrics for the architectural quality of Internet businesses, *Information Systems Research* 13 (3) (2002).
- [23] J. Lee, H.R. Rao, A study of customers' trust in government-to-customer online services, *Proc. of the 9th Americas Conference on Information Systems*, Association of Information Systems, Tampa, FL, USA, 2003.
- [24] J. Lee, H.R. Rao, S. Braynov, Effects of public emergency on citizens' usage intention toward e-Government: a study in the context of war in Iraq, *Proc. of The 24th International Conference on Information Systems*, Association of Information Systems, Seattle, WA, USA, 2003.
- [25] J. Lee, D.J. Kim, H.R. Rao, An examination of trust effects and pre-existing relational risks in e-Government services, *Proc. of The Eleventh Americas Conference on Information Systems*, Association of Information Systems, Omaha, NE, USA, 2005.
- [26] R.C. Mayer, J.H. Davis, F.D. Schoorman, An integration model of organizational trust, *Academy of Management Review* 20 (3) (1995).
- [27] D.H. McKnight, L.L. Cummings, N.L. Chervany, Initial trust formation in new organizational relationships, *Academy of Management, The Academy of Management Review* 23 (3) (1998).
- [28] D.H. McKnight, V. Choudhury, C. Kacmar, Developing and validating trust measures for e-commerce: an integrative typology, *Information Systems Research* 13 (3) (2002).
- [29] V.-W. Mitchell, Consumer perceived risk: conceptualisations and models, *European Journal of Marketing* 33 (1/2) (1999).
- [30] G.C. Moore, I. Benbasat, Development of an instrument to measure the perceptions of adopting an information technology innovation, *Information Systems Research* 2 (3) (1991).
- [31] J.W. Palmer, Web site usability, design, and performance metrics, *Information Systems Research* 13 (2) (2002).
- [32] PewInternet, How Americans used the Internet after the terror attack, http://www.pewinternet.org/reports/pdfs/PIP_Terror_Report.pdf.
- [33] PewInternet, Counting on the Internet, http://www.pewinternet.org/reports/pdfs/PIP_Expectations.pdf.
- [34] PewInternet, PewInternet project data memo, http://www.pewinternet.org/reports/pdfs/PIP_Preparedness_Net_Memo.pdf.
- [35] PIP, The Internet and the Iraq War, *Pew Internet & American Life Project*, 2003.
- [36] G. Pires, J. Stanton, A. Eckford, Influences on the perceived risk of purchasing online, *Journal of Consumer Behaviour* 4 (2) (2004).
- [37] J.W. Pratt, Risk aversion in the small and in the large firm, *Econometrica* 32 (1964).
- [38] F. Ramsey, *Truth and probability, The Foundations of Mathematics and Other Logical Essays*, Routledge & Kegan Paul, London, 1931.
- [39] L.J. Savage, *The Foundations of Statistics*, Wiley, New York, 1954.
- [40] P. Sparks, R. Shepherd, Public perceptions of food-related hazards: individual and social dimensions, *Food Quality and Preference* 5 (3) (1994).
- [41] A. Tversky, Elimination by aspects: a theory of choice, *Psychological Review* 79 (1972).
- [42] J.E. Urbany, P.R. Dickson, W.L. Wilkie, Buyer uncertainty and information search, *Journal of Consumer Research* 16 (1989).
- [43] V. Venkatesh, M.G. Morris, G.B. Davis, F.D. Davis, User acceptance of information technology: toward a unified view, *MIS Quarterly* 27 (3) (2003).
- [44] J. Vijayan, Fed agencies get a D+ in computer security, *Computerworld* 39 (8) (Feb. 21 2005).
- [45] M.E. Whitman, H.J. Mattord, *Principles of Information Security*, Thomson Course Technology, Canada, 2003.
- [46] W.A. Wulf, Y.Y. Haimes, T.A. Longstaff, Strategic alternative responses to risk of terrorism, *Risk Analysis* 23 (3) (2003).



JinKyu Lee is an Assistant Professor of MSIS in the William S. Spears School of Business at Oklahoma State University. He holds a Ph.D. in Management Information Systems (2006) from University at Buffalo, USA, a Masters degree in Information Systems (1999) from Griffith University, Australia and a Bachelors degree in Business Administration (1996) from Yonsei University, Korea. His current research interest includes Privacy and Security Risks, and

Service Performance in the e-Service area, Diffusion of Information Assurance Practice and IT/Firm Performance, Information Security Workforce Development, and Inter-organizational Secure Knowledge Management Systems. He has published refereed journal and conference articles in CACM, ICIS, AMCIS, ECEG, Springer Lecture Notes in Computer Science and has been involved in several NSF, NSA, and DoD funded research/educational projects in e-government and information assurance areas.



H. Raghav Rao is a Professor at the Management Science and Systems department in the School of Management and an Adjunct Professor at the Computer Science and Engineering department, University at Buffalo, NY. He holds Ph.D. (1987) degree from Krannert Graduate School, Purdue University, M.B.A. (1981) from University of Delhi, India, and B. Tech.(1979) from Indian Institute of Technology, India.

His research interest includes Information and Decision Theory, e-Government and e-Commerce, Information Assurance, and Economics of Information, and has published over 70 refereed research articles in academic conferences and journals. He is a Co-Editor-in-Chief of a new journal by Springer, *Information Systems Frontiers: A Journal of Research and Innovation* and an associate editor of *Decision Support Systems*, *Information Systems Research*, *IEEE Transactions on Systems, Man and Cybernetics, Part A*. He has also co-guest edited numerous special issues for leading journals including *Decision Support Systems*, the *Communications of the ACM*, the *Annals of Operations Research*.