Risk of Terrorism, Trust in Government, and e-Government Services: An Exploratory Study of Citizens' Intention to use e-Government Services in a Turbulent Environment[1]

JinKyu Lee and H. Raghav Rao
Management Science and Systems
University at Buffalo
Buffalo, USA

YCISS Working Paper Number 30
January 2005

The YCISS Working Paper Series is designed to stimulate feedback from other experts in the field. The series explores topical themes that reflect work being undertaken at the Centre.

[1] This paper is based on the authors' preliminary work presented at the ICIS 2003, Seattle, USA. The research of the second author has been supported in part by NSF under grants 0423014, 0420448, 0417095. 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 Professor Svet Braynov for his help during the initial phase of the research. The second author would like to thank Dr. David Dewitt for his support during the Fulbright fellowship. We also thank the anonymous referee for critical comments.

Abstract

For the last several years, US citizens have been experiencing severe threats of terrorism. While such threats can significantly impact important factors for effective government operations such as citizens' information demand and attitude toward the government, little is known about their potential effect on citizens' acceptance of e-Government services. In order to fill this gap, this study examines the effects of perceived risks of terrorism and trustworthiness of the government, on citizens' e-Government usage intentions. The data was collected through two surveys with a one-year interval: during and after the war in Iraq. The analysis revealed that citizens' e-Government usage intentions can be significantly influenced by perceived risks of terrorism and trustworthiness of the supreme government, as well as other factors suggested by previous research. These relationships appear to vary depending on the domain and the type of the particular e-Government service. Other findings and future research needs are also discussed.

Introduction

For the last several years, many government organizations have been trying to transform into a more efficient and effective organization by adopting new technologies, especially the Internet. At the federal level, e-Government initiatives have developed various web-based public services such as FirstGov.gov, a gateway to more than 180 million web pages from federal and state governments, Disasterhelp.gov, an information source for about 15,000 emergency managers, Grants.gov, a government grant search and application tool for more than $360 billion in annual grants, and IRS.gov that offers free on-line tax filing services already used by more than 3.4 million taxpayers [1, 2]. In the 2003 fiscal year, $4,967,500 was available for e-Government development [3]. 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 [4]. Nevertheless, the increased public concern over terrorism and information security of US citizens is presenting new hurdles as well as opportunities to for government efforts to leverage efficient technologies.

According to a recent large-scale poll, half of Americans are worried about possible terrorist attacks, including cyber-attacks on social infrastructure [5]. With the increased role played by the US government in the international community, the threat is unlikely to be dissolved in the near future [6]. Even before the 9/11 attacks, information security and privacy were already the biggest public concerns in e-Government development [7]. Meanwhile, US citizens' dependency on the Internet for government information and services, especially those related to national emergency, have greatly increased [8]. 56 percent of American Internet users went online for Iraq war-related information, such as how the war was developing over time and how to prepare for possible terrorist attacks. During the war, US government sites were a major information source, attracting 15 percent of American Internet users. Also, 17 percent of American Internet users identified the Internet as the primary information source or communication medium, a big leap from the 3 percent immediately before the 9/11 incidents [9]. 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 of online government information [10]. [1]

These conflicting pressures among factors such as technology utilization, external threat (i.e., terrorism) and security concerns, demands for government information, and government control for public information can have much influence over citizens' e-Government acceptance decisions and behaviour, which in turn can confuse e-Government initiatives in understanding why some e-Government services are readily accepted while some others fail to attract citizens. Therefore, an important and urgent task assigned to e-Government initiatives in this turbulent environment is to *understand how citizens' perception of the risky environment affects their acceptance of e-Government services* and to secure stable functioning of e-Government operations. What are the risks that citizens are concerned with in the context of e-Government service use? When citizens face a high risk, will they rely on safety information available on an e-Government website? Will they provide personal information to an e-Government website under such a risk? If not, how can e-Government agencies improve their services and realize the potential benefits of information technology? Understanding public perceptions of risk and interaction with public websites are critical steps to effective risk-communication practice [11] and networked communities [12]. However, few researchers have explored factors influencing citizens' risk perception and acceptance of e-Government services, and virtually nothing is known about the effect of external threats.

This study has a twofold objective. First, the paper, based on user acceptance theories in the Management Information Systems (MIS) field, synthesizes a model that can explain citizens' e-Government usage intentions. Second, it empirically examines the effects of various types of risks in the e-Government service context, collectively and in groups of functional domain. The types of risks include:

- risks from uncertain future behaviour of the supreme government[2] and e-Government agencies,
- security and privacy risk from the Internet, and
- threats to public safety coming from the physical world.

The last category of risks can include various threats to the safety of the general public posed by a strategic adversary (e.g., enemy in a war, terrorists) or a natural disaster (e.g., hurricane, earthquake, flood, epidemic disease), but this study focuses on the 'risk of terrorism.' For the first two types of risks – risks regarding government authorities – we use the concept of 'trustworthiness' as the counter concept of corresponding risks. The third risk from the Internet is also referred to, in a reverse manner, as 'structural assurance' in order to contextualize our study within the framework of previous literature. Accordingly, we integrate and extend theoretical models from traditional technology acceptance theories and e-commerce research to include relevant concepts in the context of e-Government services. The resulting model can take into account the effect of each risk as well as other factors influencing citizens' intention to use e-Government services. Also, the model will reveal differences of citizens' intention formation between terrorism related and unrelated e-Government services.

The invasion in Iraq and 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 a 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 had to raise the national terrorism threat level to High (level orange). We conducted the first questionnaire survey when the Iraq war was dynamically developing and the alert level was orange, and the second one exactly one year later, when the alert level was lowered to yellow, yet the news reported US casualties on a daily basis.

[1] http://www.ombwatch.org/article/articleview/213/1/1/

[2] By supreme government, we mean the decision/policy maker of a national government. In the US government, this concept can be understood as the federal level legislative bodies backed by some executive bodies.

Theoretical Background

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

Intention to use e-Government Services

The motivations of this study (i.e., promoting e-Government use and assuring dependable e-Government services in a public emergency situation) are in line with the concept of information system success at both user [13] and organizational [14] levels. In this study, we combine both perspectives and propose to use the concept of 'intention to use e-Government website' to measure both user satisfaction and achievement of organizational objectives. A government can be understood as either a protector or a controller of its citizens. For the protector role, citizens are both consumers of the protection service and sensors (i.e., eyes and ears[3]) of the protector. 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, while the government's performance as a protector is largely dependant on its capabilities to gather intelligence and mobilize citizens through e-Government systems. Therefore, citizens' willingness to be informed by, follow directions of, and provide information to e-Government can reflect the success of e-Government. Based on this viewpoint, we use two intention measures: citizens' *Intention to Depend on Information on an e-Government website (IDI)* and *Intention to Provide personal Information to the website (IPI)*.

The intention measure is more useful than actual usage behaviour in this context, because use of most e-Government websites is totally voluntary, and actual usage behaviour, especially such behaviour as providing leads and tips of a terrorist attack, does not occur often. Also, we assume that current e-Government facilities are still in their primitive forms and do not provide every possible service that citizens need. Therefore, intention measures are useful proxies of future use [15] in our study context.

Direct Determinants of e-Government Usage Intentions

Factors that determine or predict user acceptance of information systems have been one of the most intensively examined topics in MIS studies. Based on the well established traditional IT acceptance theories [16, 17] and the newer e-commerce trust models [18, 19], we contend that citizens' acceptance of e-Government services can be understood in terms of two dimensions: direct utility value and risk reduction.

Perceived Usefulness of e-Government Website

The Technology Acceptance Model (TAM) [17, 20] contends that potential user's acceptance and use of an information system can be best explained by perceived usefulness, perceived ease of use, and subjective norm. This model was built on the Theory of Reasoned Action (TRA) that views human behaviour as a direct function of behavioural intentions, and beliefs as determinants of the intentions [21,

[3] http://www.msnbc.msn.com/id/4861685/

22]. In TAM, perceived usefulness was defined as "the degree to which a person believes that using a particular system would enhance his or her job performance" [17 p.320], which explicitly reflects the utility value that directly comes from system use. The significant effect of perceived usefulness has consistently been found in most empirical studies, while users' experience [23, 24] and voluntariness [25, 26] diminish the effects of ease of use and subjective norm, respectively. Many other IT use studies also reflect utility value as a major determinant of IT use/usage intention, in the form of task support and future value [27], superior functionality [28, 29], instrument for extrinsic rewards [30], or job performance [31]. Venkatesh *et al*. provide a comprehensive summary of the IT acceptance studies centred around utility value [16]. Similar to the private sector counterpart, citizens' acceptance of an e-Government service will also be affected by the utility value of the service. However, it is difficult to predefine the type of benefits from e-Government services that provides high utility value. Unlike a user of an organizational information system, citizens can selectively use a wide range of e-Government services that provide heterogeneous functions (e.g., supporting tax filing tasks, introducing activities of a government agency, disseminating public safety information, etc.), depending on their temporal needs. Also, one e-Government website can serve multiple functions (e.g., a gateway to another e-Government service, imposing control over citizens, or providing public services) which are loosely coupled yet influencing each other. In this case, measuring or comparing the service-specific utility of an e-Government function with another is neither meaningful nor desirable. Therefore, we re-conceptualize the term "perceived usefulness" as the general belief of an e-Government website visitor regarding the potential utility of the information and functionality of the website, rather than adopting Venkatesh *et al*.'s concept of performance expectancy that focuses on productivity, competitive advantage, and external rewards in workplace [16]. H1a and H2b in the conceptual model (Figure 1) and Table 1 show the hypothesized positive relationships between perceived usefulness and intentions to use e-Government website.

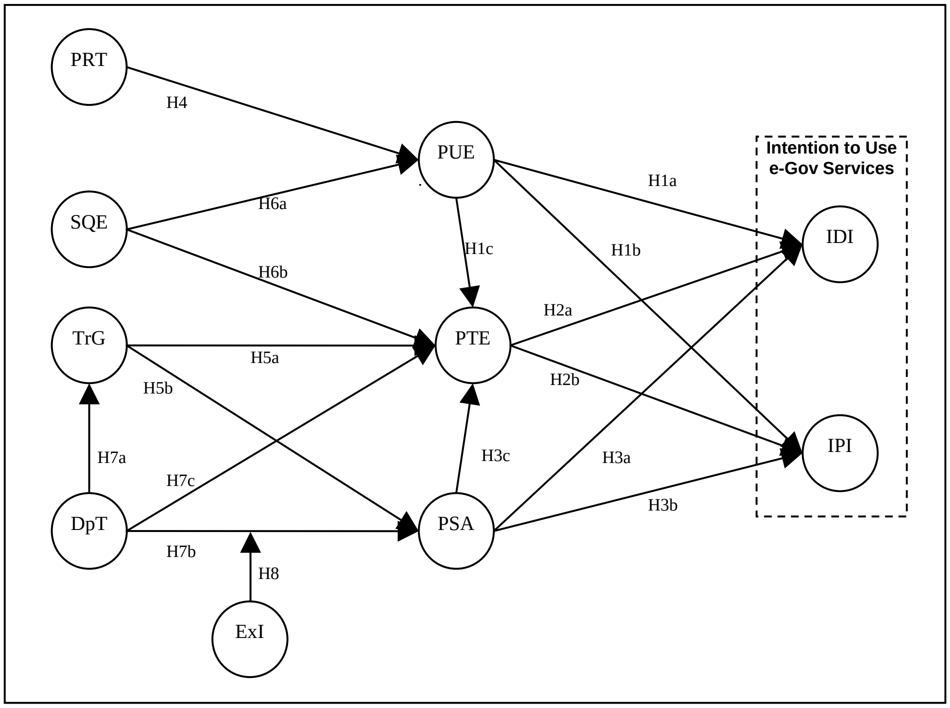

Figure 1. Conceptual Model

We also hypothesize a positive effect of perceived usefulness on perceived trustworthiness (H1c). Gefen *et al*. suggested the same relationship in the opposite direction based on social exchange theory [32]. According to their argument, absence or incompleteness of contracts in social relationships (i.e., online shopping) requires trust to supplement online customers' subjective expectation on the resulting utility. While such an effect is certainly possible, it is also logical to expect bidirectional feedback loop between the two constructs. Gefen *et al*.'s study was mainly concerned with discrete spot transaction relationships where potential customers assess the utility of an online transaction at the point of purchasing decision, and the transaction ends by receiving the ordered items. However, e-Government websites are a result of government operations supported by taxpayers' money. In this sense, perceived usefulness of an e-Government website is an indicator of the website operators' performance. In our cases (i.e., NYSOPS, FBI and NYDMV), citizens would assess the government agencies' operational performance based on what they found on the websites, which may require them to revise their previous beliefs in the agencies' trustworthiness. This relationship is also parallel to the relationship between government performance and government authority. Authority refers to the power or rights of a government honoured by its citizens. From the social exchange perspective, the legitimacy of the power is conferred on government in exchange for citizens' satisfaction on the government performance [33, 34]. When an e-Government website does not provide useful services, citizens' beliefs in the website operator's benevolence, integrity, and competence will decrease, which will undermine the operator's authority.

Table 1. Hypotheses

Hypotheses	Symbol
H1a. Perceived usefulness of an e-Government website (PUE) positively affects citizens' intention to depend on information on the website (IDI).	PUE → IDI (+)
H1b. Perceived usefulness of an e-Government website (PUE) positively affects citizens' intention to provide personal information to the website (IPI).	PUE → IPI (+)
H1c. Perceived usefulness of an e-Government website (PUE) positively affects perceived trustworthiness of the e-Government website (PTE).	PUE → PTE(+)
H2a. Perceived trustworthiness of an e-Government website (PTE) positively affects citizens' intention to depend on information on the website (IDI).	PTE → IDI (+)
H2b. Perceived trustworthiness of an e-Government website (PTE) positively affects citizens' intention to provide personal information to the website (IPI).	PTE → IPI (+)
H3a. Perceived structural assurance of the Internet (PSA) positively affects citizens' intention to depend on information on the website (IDI).	PSA → IDI (+)
H3b. Perceived structural assurance of the Internet (PSA) positively affects citizens' intention to provide personal information to the website (IPI).	PSA → IPI (+)
H3c. Perceived structural assurance of the Internet (PSA) positively affects perceived trustworthiness of e-Government websites (PTE).	PSA → PTE(+)
H4. Perceived risk of terrorism (PRT) positively affects perceived usefulness of e-Government websites (PUE).	PRT → PUE(+)
H5a. Trust in supreme government (TrG) positively affects perceived trustworthiness of e-Government websites (PTE).	TrG → PTE(+)
H5b. Trust in supreme government (TrG) positively affects perceived structural assurance of the Internet (PSA).	TrG → PSA(+)
H6a. System quality of an e-Government website (SQE) positively perceived usefulness of the e-Government website (PUE).	SQE → PUE(+)
H6b. System quality of an e-Government website (SQE) positively perceived trustworthiness of e-Government websites (PTE).	SQE → PTE(+)
H7a. Disposition to trust (DpT) positively affects trust in supreme government (TrG).	DpT → TrG(+)
H7b. Disposition to trust (DpT) positively affects perceived structural assurance of the Internet (PSA).	DpT → PSA(+)
H7b. Disposition to trust (DpT) positively affects perceived trustworthiness of e-Government websites (PTE).	DpT → PTE(+)
H8. Experience with the Internet (ExI) has a negative moderating effect on the relationship between DpT and PSA (H7b)	DpTxExI → PSA(-)

Relational Risk and Perceived Trustworthiness of e-Government Website

This study integrates an e-commerce trust model with the traditional theories of IT acceptance and use. Prior literature has suggested trust as a critical success factor for e-commerce [19, 32, 35]. Mayer *et al*. 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" [36 p.712]. Their organizational trust model suggests that trust be determined by a trustor's perception on the trustee's trustworthiness (i.e., ability, benevolence, and integrity) and the trustor's propensity to trust. According to the model, trust leads the trustor to take a risk in the relationship with the trustee. McKnight *et al*. extended and applied this model to the e-commerce context [18, 19]. "Trusting beliefs" in their e-commerce trust model are equivalent to a trustor's beliefs in the trustee's trustworthiness and "trusting intention" can be interpreted as the trustor's willingness to engage in the risky relationship with the trustee. This concept of trusting intention is analogous to TAM's concept of "intention to use" in our study context. Some studies based on this e-commerce trust model provided empirical support for the validity of measurement model [19] and the relationship between trusting beliefs and trusting intention [37]. In a recent paper, Gefen *et al*. also combined perceived usefulness, ease of use, and trust as determinants of intended use and demonstrated a significant effect of trust on the dependent measure [32]. As this relational trust allows people to dismiss or overcome the risk of e-commerce vendors' future misbehaviour, perceived trustworthiness of an e-Government website agency can enable citizens to depend on the information from or disclose sensitive information to the agency. As some e-Government services are jointly provided by multiple government organizations or government contractors, we use the term 'e-Government website (and its operator)' to generally represent the e-Government side entities related to an e-Government website-citizen interaction. H2a and H2b (Table 1) hypothesize the positive (negative) relationships between perceived trustworthiness of (relational risk from) e-Government website and e-Government usage intentions.

Risk from the Internet and Perceived Structural Assurance

Mayer *et al*. [36] argued that situational risks that are external to a particular relationship need to be analyzed separately from trust because these risks are not related to the trustee's behaviour. In addition to the relationship specific risk discussed in the previous section, there are two types of situational risks that can influence citizens' e-Government use: risks from technical and legal vulnerability of the Internet environment (i.e., threat of hackers and Internet scam) and risks from the physical environment at a particular time (e.g., threat of terrorism, natural disaster). These risks are external to the relationships between citizens and e-Government websites and, therefore, must be separately analyzed.

The e-commerce trust model suggests that institution-based trust have a direct effect and an indirect effect, through trusting beliefs, on trusting intention [19]. Institution-based trust consists of situational normality which reflects a trustor's perception on the situation where everything seems normal or in the right order, and *structural assurance*, which refers to the beliefs that legal and technological safeguard are in place to protect the trustor. From this definition, we notice that the structural assurance concept reflects the situational risk of the Internet environment, while the situational normality may compound the appearance of an e-Government website and the conditions of the Internet and the physical environments. Thus, we separate structural assurance and use to measure the risk of Internet Environment in a reverse term. Our notion of structural assurance is narrower than Gefen *et al*.'s (2003) recent manifestation in that we focus on citizens' perception of the existing technology and legal infrastructure, while Gefen *et al*.'s construct looked at website-specific components (i.e., 3rd-party seal, 1-800 number, statement of guarantees, and hyper-link with reputable websites). Having this narrower focus, perceived[4] structural assurance of the Internet in our study context will have the same effect on usage intention as in the e-commerce context because the concept is a counter-measure of the risk general to the Internet and legal jurisdiction, which are over and beyond website operators' control or discretion. Previous research on citizens' use of the Internet suggest that technological robustness of the Internet increase citizens' use of the Internet in an emergency. A report from such a survey shows that, 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 [38]. Likewise, those who could not access the major Internet news sites (e.g., www.cnn.com, www.msnbc.com) immediately after the 9/11 because of the temporal bottleneck may not want to depend on e-Government websites for time-critical emergency services. These effects are hypothesized as H3a and H3b (Table 1). Although our structural assurance does not include the above mentioned website-specific components, there has been no empirical evidence that general perception of Internet infrastructure does not affect the perceived trustworthiness of a website. As an exploratory study, we include a positive relationship in our model and empirically test the effect (H3c).

Effects of External Threat

The second type of situational risks, "risks from the physical environment at the particular time," refers to the war in Iraq and threats of terrorism caused by the war in our study. In contrast to the other types of situational risk (i.e., risk from the Internet), this external threat of terrorism affects the physical environment of citizens, as opposed to the Internet environment. We hypothesize that the external threat positively affects perceived usefulness (H4), thus have an indirect positive effect on the usage intentions. This effect on the usefulness can be explained by the concept of subjective uncertainty and expected utility [39, 40]. Subjective expected utility (SEU) assumes that there is no agreed-upon likelihood of possible outcomes [41] and expressed as:

> $\mathrm{SEU}(X) = \sum p(s)u(x(s))$, where $p(s)$ is the subjective probability of an outcome state (s), $x(s)$ is the consequence of the purchase/action of (X) at the outcome state (s), and $u(x(s))$ is the utility of the consequence at the state ($x(s)$).

As assumed in SEU, there are a multiple number of states where an individual becomes a victim of a terrorist attack (e.g., killed by a terrorism, losing loved one, having financial damage, etc.), and the probability of the states are unknown. For each state, using an e-Government service will have different utility. For example, knowing an evacuation plan for a bio-terrorism will be of a great help when such an incident happens, and renewing a driver's license online would be very useful when government buildings became the targets of an anthrax attack. Therefore, increased external threats will have a positive effect on perceived usefulness by increasing the subjective probability of risky states ($p(s)$) and selectively increasing the utility of some e-Government services (i.e., anti/counter-terrorism services, online transaction with high-profile government agencies) at the risky states ($u(x(s))$). Furthermore,

[4] We use the term 'perceived' to emphasize that situational assurance is also a belief of citizens and that our construct is different from Gefen *et al*.'s (2003) construct measured by more objective website components.

anti/counter-terrorism websites not only provide information on how to cope with possible or existing danger, but also provide information about the likelihood of possible risks. For example, the Department of Homeland Security website provides the current level of terrorist threats and intelligence on possible terrorism, which can reduce the ambiguity in the probability assessment. Ambiguity aversion is a frequently observed behaviour in risky decision making [42], and is found to increase as the range of possible probability increases [43] or the probability of negative outcome increases [44]. Therefore, a perceived risk of terrorism will result in a higher demand, and thus, increase perceived usefulness of the information that helps citizens to accurately assess the probability of the terrorist attacks. H4 in Table 1 presents the positive effect of perceived risk of terrorism on perceived usefulness.

Effects of Trust in Supreme Government

The last category of risk relevant to the e-Government context comes from uncertain future behaviour of the supreme government. Although government organizations, including e-Government agencies, have autonomous power and rights to some extent, every government organization is subject to the supreme government's control, a situation where the trustworthiness of the supreme government can be transfered to e-Government agencies. 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, which was vaguely defined, and allows the President and the DHS Secretary to decide the use and reuse of such information given to states and localities.[5] For another example of such organizational control, Attorney General John Ashcroft, in 2001, instructed federal agencies to hold back government information, using the exemption clauses in Freedom of Information Act (FOIA). Consequently, the General Accounting Office (GAO) reported a significant reduction of publicly available information resulting from the instruction.[6] The USA PATRIOT Act has conferred a great level of authority to federal officials since 2001, which has increased concern about civil rights, and yet, additional legislation – i.e., Patriot II (Domestic Security Enhancement Act of 2003),[7] Intelligence Authorization Act of 2005[8] –are further threatening citizens' privacy and freedom.

In addition to its organizational control, the trustworthiness of supreme government can influence that of e-Government websites through a cognitive categorization processes. The concept of the cognitive categorization process was introduced in e-commerce trust studies by McKnight *et al*. [18]. According to their explanation, people tend to trust an unfamiliar entity if the entity is a member of a reputable organization and vice-versa (reputation categorization). Gefen *et al*. [32] also recognized this cognitive process as an antecedent of trust (i.e., cognition-based trust antecedents). Nevertheless, they ruled out the effects of cognition-based trust antecedents in non-initial relationships. Although the sample sites (i.e.,

[5] http://www.ombwatch.org/homeland/OMBW-SBU.pdf, http://www.openthegovernment.org/article/articleview/49/1/16/
[6] http://www.openthegovernment.org/article/subarchive/19/
[7] http://www.publicintegrity.org/dtaweb/downloads/Story_01_020703_Doc_1.pdf
[8] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=s2386ris.txt

NYDMV, FBI, NYDMV) are of fairly familiar government agencies, we include this relationship in our model because Gefen *et al*.'s study did not conduct empirical tests on the relationship, and because we aim to build a model that can be applied generally to various e-Government websites.

As the highest legislative and executive body, the supreme government can also affect the perceived structural assurance of the Internet by imposing regulations to industries. Because structural assurance reflects legal safeguards by definition, the citizens' belief that the supreme government will protect their online activity by providing appropriate regulatory measures will increase their structural assurance belief. The Children's Online Privacy Protection Act (Coppa),[9] the Gramm-Leach-Bliley Act[10] for financial the industry, and the Health Insurance Portability and Accountability Act (HIPAA)[11] exemplify such influence. Based on the above discussion, we hypothesize positive effects of trust in supreme government on perceived trustworthiness of e-Government website (H5a) and on perceived structural assurance (H5b).

Control Variables

In order to avoid a spurious correlation, we include three control variables in our model. Previous research suggested that the qualitative properties of a website such as organization/navigational quality, retrieval speed, and interactivity (Palmer 2002; Kim *et al*. 2002; McKinney *et al*. 2002) are important factors for e-commerce website success. *System quality of an e-Government website*, in our study, captures those various system properties specific to an e-Government website. From a potential users' standpoint, system quality can represent a dimension of the product/service quality itself (e.g., easy to understand/navigate contents) as well as the quality of the product delivery channel (e.g., easy to complete and interactive online applications/transactions, fast response of web server), both of which are direct sources of the utility value. Also, a high quality system shows website users that the website operator cares for them and has the competence to carry out online services [32, 45, 46]. McKnight *et al*. also included a similar concept (i.e., perceived site quality) in their e-commerce trust model as a control variable [19]. They hypothesized that perceived site quality can positively influence both perceived trustworthiness (i.e., trusting beliefs) and trusting intentions (i.e., willingness to depend and subjective probability of depending). However, their model did not take into account the effect of utility value, and it is difficult to expect that people will (intend to) use a website just because its system quality is good. Thus, we assume that usefulness perception fully mediates the effect of perceived system quality on the intention to use the website. Including system quality as a common cause of perceived usefulness and trustworthiness can also reduce the risk of spurious correlation between the two constructs (and thus of H1c). These relationships are hypothesized as H6a and H6b in Table 1 and Figure 1.

Disposition to trust has been suggested to have positive effects on other trust factors (i.e., institution-based trust, trusting beliefs, trusting intentions) [19, 46], conditional to individuals' direct experience with the trustee [32]. That is, although this personal disposition is relatively stable and

[9] http://www.ftc.gov/opa/2000/04/coppa1.htm
[10] http://www.ftc.gov/privacy/glbact/oldstuff_donotuse/index.html
[11] http://www.hhs.gov/ocr/hipaa/

influential to the individual’s beliefs in general, the effects are overridden by trustee-specific experience [47]. When the effect exists, not including the disposition may result in spurious correlations between the other trust factors. Therefore, we include disposition to trust in our model where trust in supreme government and perceived situational assurance in the Internet are hypothesized to affect perceived trustworthiness of an e-Government website. Also, we include *experience with the Internet* as a moderating variable between disposition to trust and perceived structural assurance of the Internet. Because we hypothesize that structural assurance beliefs, as a counter-measure of Internet risks, have direct and indirect effects on the usage intentions, understanding the effect of Internet experience will provide an important insight on how Internet savvy and novice users perceive risk from the Internet. The positive effects of disposition to trust on trust in government, structural assurance, and perceived trustworthiness of e-Government website are hypothesized as H7a, H7b, and H7c respectively (Table 1 and Figure 1). The experience effect on structural assurance is denoted as H8. This relationship, however, is separately implemented as a direct effect (H8a) and an interaction effect with disposition to trust (H8b) in the PLS structured model (Table 8 and Figure 2, 3, 4).

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 in time. The first survey was conducted in April 2003 when the second Iraq war was dynamically developing 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 end of the war. The second survey was designed to achieve several research goals. As one of the research objectives is to understand how to secure stable functioning of e-Government services when risk of terrorism exists, the survey data should capture citizens’ perceptions 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 provides useful insights about trends in public perceptions and intentions, especially on issues of trust in supreme government.

The survey was conducted in a large north-eastern US university located near the Canada-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 Vehicle (NYDMY). These websites were selected to represent two levels (i.e., federal and state) and two roles (i.e., protection and control) of e-Government authorities. These questionnaires were randomly distributed to 240 students enrolled in an undergraduate-level management course and yielded 177 responses (73.8 percent). Subjects were required to visit and examine the informational content and transaction functions of a specified e-Government website before answering the questionnaire. The same procedure[12] was followed during the second survey, which was administered to 219 undergraduate-level students in a

[12] We only used two versions of 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.

management course. 137 completed questionnaires were returned with 62.6 percent response rate, and the Department of Homeland Security's terrorism threat advisory level was 'elevated' (level Yellow) during the second survey period.

The measurement and structured model was analyzed using PLS Graph v3, a partial least square based Structural Equation Modeling (SEM) tool. PLS is an appropriate tool for relationship testing in a theory development stage. As this study applies many theoretical relationships originally developed in a private-sector environment and political world to a new context of e-Government, PLS provides better insight for further refinement of our model. A detailed procedure is described in the Data Analysis section.

Sampling and External Validity

As 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 cohort-groups that share the same demographic and psychological characteristics [48]. This sampling method provides a homogeneous group of subjects, in our case, young, well educated, and Internet literate. The average age of the respondents was 21.4 years old, all of them were in a bachelor degree program, and 95 percent of them had been using the Internet for more than 3 years. McKnight *et al.* argued that this kind of student sample can be a good proxy of the e-consumer population who are generally younger and more highly educated than average consumers [19]. A citizen poll also found that American Internet users under the age of 30 or with college educations, utilized the Internet the most in relation to the Iraq war [49]. 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 enables us to circumvent compounding effects from different demographic groups. As 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 provides clearer picture of the decision pattern and a rigid step for future theory extension.

Although studies using student subjects have often been criticized for low external validity [50], there were several reasons we believed that student sample would not compromise the validity and would indeed be beneficial to 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 external threats as US residents, and the younger age range could lower the risk aversion factor, which would make the study more conservative. Furthermore, students are not only legitimate users, but are also the most likely prospective users of our e-Government website samples. NYDMV's online driver's license renewal service is a featured link on the FirstGov,[13] an acclaimed US government portal to 180 million federal and state e-Government web pages [51]. Driver's license and car registration are applicable to anyone in the US, and in fact, the DMV is one

[13] http://www.firstgov.gov/ or http://www.firstgov.com/

of the first US government agencies to deal with for many college students, including international students. The NYSOPS and the FBI are representative anti/counter-terrorism government authorities, at state and federal level respectively. For these reasons, our student sample represents a large portion of potential e-Government website users and has high external validity.

Measurement Items

Most of the measurement items included in the questionnaires came directly from or were adapted from previous research. The two types of e-Government usage intentions, intention to depend on information on the e-Government website (IDI) and intention to provide personal information to the e-Government website (IPI), were each measured by four indicators. They were originally developed in an e-commerce trust measure study [19] and modified to reflect the specific context of the websites in question. Perceived usefulness of an e-Government website (PUE) used three items that were developed based on the perceived usefulness and relative advantage measures in the IT acceptance and use literature [17, 20, 28]. Perceived trustworthiness of an e-Government website (PTE) measure was adapted from McKnight *et al*.'s e-commerce trust measurement model [19] with minimal changes in the wording. While the original measure for trusting beliefs has three sub-constructs (i.e., benevolence, integrity, and competence), PTE is measured by four items: three items from the three different sub-constructs, and one for competence in online service. The three-item measures for perceived structural assurance of the Internet (PSA) and disposition to trust (DpT)[14] are directly from the structural assurance measure and disposition measure respectively also developed in the e-commerce trust model. Trust in supreme government (TrG) was measured by three items originally used to measure political trust in political science literature. System quality of an e-Government website (SQE) is an emergent construct that had three formative indicators. Each item represents heterogeneous website system properties that have been identified as important quality factors in e-commerce and website design literature [52, 53]. The three-item measures for perceived risk of terrorism (PRT)[15] and experience with the Internet were newly developed for this study as there was no widely accepted measure. Measurement items for the FBI website are presented in Table 2.

Table 2. Measurement Items. (FBI version: *WebSite X* = www.fbi.gov)

Intention to Use e-Gov Services
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 in *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.

[14] DpT measure originally had 4 items, but one item (DPT4 in Table 2) was dropped due to low convergent validity in the measurement model testing.

[15] PRT measure originally had 4 items, but one item (PRT4 in Table 2) was dropped due to low convergent validity in the measurement model testing.

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.

Perceived Usefulness of e-Gov Website

PUE1. I find using *WebSite X* useful.

PUE2. *WebSite X* provides useful information.

PUE3. Using *WebSite X* can be more effective than dealing with real people for the same service.

Perceived Trustworthiness of e-Gov Website

PTE1. *WebSite X* (and its operator) is interested in my well-being, not just its own.

PTE2. *WebSite X* would keep its commitments.

PTE3. *WebSite X* is capable and proficient in public security service.

PTE4. *WebSite X* is capable and proficient in online service.

Perceived Structural Assurance of the Internet

PSA1. The Internet has enough safeguards to make me feel comfortable using it to transact sensitive information.

PSA2. I feel assured that legal and technological structures adequately protect me from problems on the Internet even in an emergency.

PSA3. I feel confident that encryption and other technological advances on the Internet make it safe for me to do business there.

Perceived Risk of Terrorism

PRT1. The [war | US stationary troops] in Iraq has created an emergency in the US.

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.

PRT3. The [war | tension between the US and Iraq] makes me concerned for my safety in the US.

PRT4. I watch or read news about US activities in Iraq as much as I can.**

Trust in Supreme (Federal) Government

TrG1. Most politicians in this country can be trusted to do what they think is best for the country.

TrG2. I usually have confidence that the US government will do what is right.

TrG3. The US government will ensure that everybody who wants to work can find a job.

System Quality of e-Gov Website***

SQE1. *WebSite X* is effectively organized.

SQE2. *WebSite X* provides significant user interaction.

SQE3. In *WebSite X*, the speed of information display was too slow*.

SQE4. *WebSite X* provides feedback mechanisms.

Disposition to Trust

DpT1. In general, people really do care about the well being of others.

DpT2. In general, most folks keep their promises.

DpT3. Large majority of professional people are competent in their area of expertise

DpT4. I usually trust people until they give me a reason not to trust them.**

Experience with the Internet

ExI1. Number of transactions you have provided your credit card number over the Internet to an online entity for the last one year:

ExI2. Number of transactions you have provided your personal information (e.g., social security number, drivers license number) over the Internet to an online entity for the last one year:

ExI3. How many hours per week do you spend on the Web?

* Reverse-worded item.

** Dropped item for low reliability reason.

*** Emergent construct with formative indicators

Data Analysis

Table 3. 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

After data cleaning,[16] the resulting 269 cases (Table 3) 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 datasets should be the (length of) existence that the subjects perceived the abnormal event (i.e., the war between the US and Iraq) and the consequent perception of terrorism risk and trust in supreme government. The two groups seemed to share the same demographic characteristics in terms of the average length of US residency and 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 differences within one-year gap. Table 4 shows detailed group demographics, including independent T-test results.

The measurement model was tested using PLS. In the reliability and validity testing stage, two items (refer to Table 2) were dropped due to their low loadings. After the modification in the measurement model, 4 out of our 30 (13 percent) reflective indicators were below 0.7. Among those 4, one (ExI3) was about 0.59 and the other three (IDI3, IDI4, IPI4) were about 0.68.

The ideal level of standardized loadings for reflective indicators is 0.707 or higher, but 0.5 was considered to be an acceptable level for a newly developed scale or an application across disciplines [54] [55]. Therefore, we decided to retain the 4 items. Composite reliabilities for all constructs were well over the acceptable level of 0.7, and thus good convergent validity was demonstrated [56]. Discriminant validity was tested by average variance extracted (AVE) and cross-loadings. Every construct's AVE score was higher than its correlations with other constructs (Table 5). The correlations between construct scores and standardized reflective indicator values also showed that there was no significant cross-loading (Table 6).

Table 4. Sample Statistics

Characteristics	YEAR	N	Mean	t	df	Mean Difference
Age	**2003**	154	21.51	2.697**	262	0.97
	2004	110	20.55			
Education[+]	**2003**	143	3.01	7.478**	159	0.86
	2004	96	2.15			
Years in the US[+]	**2003**	155	17.361	-1.197	248	-1.0113
	2004	102	18.373			
Hours on the Web /Week	**2003**	155	17.742	-0.219	256	-0.413
	2004	103	18.155			
Expertise in Computer	**2003**	157	5.1	-1.3	265	-0.15
	2004	110	5.25			
Expertise in Web	**2003**	156	5.03	0.104	264	0.01
	2004	110	5.02			

* Significant at p<.05, ** Significant at p<.01 level
+ equal variance not assumed

[16] Cases with extremely low variance or 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. Respondents who answered any of those tester items were excluded. Obvious patterned-answers were also manually filtered out from the both datasets.

Table 5. Inter-construct Correlation and AVE Values

	IDI	IPI	PUE	PTE	PSA	PRT	TrG	SQE	DpT	ExI
IDI	0.549									
IPI	0.164	0.610								
PUE	0.384	0.229	0.663							
PTE	0.546	0.200	0.434	0.625						
PSA	0.086	0.281	0.190	0.234	0.768					
PRT	0.092	-0.021	0.126	0.123	0.009	0.593				
TrG	-0.018	0.174	0.086	0.140	0.362	-0.065	0.585			
SQE	0.376	0.032	0.492	0.414	0.141	-0.003	-0.007	N/A*		
DpT	0.148	0.063	0.270	0.259	0.338	-0.083	0.300	0.254	0.676	
ExI	0.013	0.129	0.135	-0.01	0.276	0.094	0.034	-0.037	0.025	0.534

N/A*: Emergent construct with formative indicators.

On the confirmation of acceptable reliability and validity, we tested time difference in the exogenous variables (i.e., PRT, TrG, DpT, SQE, ExI) and constructed an interaction effect variable (DpTxExI) with product indicators [57]. The time difference was tested by comparing the mean values of the exogenous construct scores calculated by PLS. We expected that perceived risk of terrorism (PRT) had been decreased during the 1 year interval, and all the others remained the same. Interestingly, the independent t-test result showed that the average level of perceived risk of terrorism was decreased but the magnitude was statistically non-significant. Instead, the level of trust in the supreme government, on average, had decreased significantly during the same period. This phenomenon may be explained by the continued conflict between the US and Islamic resistance in Iraq. Although President Bush declared the end of major combat in 1 May 2003 with the death of 138 Americans, casualty and death of American soldiers and citizens in Iraq continue, exceeding the 1,000 people on 8 September 2004.[17]

[17] http://www.msnbc.msn.com/id/5911852/

Table 6. Construct Score - Std. indicator Value Correlations : Cross-Loadings

	IDI	IPI	PUE	PTE	PSA	PRT	TrG	DpT	SQE**	ExI
IDI1	**0.795**	0.157	0.292	0.51	0.106	0.107	0.109	0.155	0.286	-0.027
IDI2	**0.807**	0.057	0.317	0.418	0.04	0.04	-0.066	0.103	0.27	0.042
IDI3	**0.67**	0.154	0.287	0.397	0.11	0.126	-0.019	0.118	0.285	0.077
IDI4	**0.681**	0.127	0.244	0.281	-0.004	0.001	-0.089	0.057	0.284	-0.051
IPI1	0.218	**0.861**	0.215	0.26	0.235	-0.008	0.12	0.016	0.137	0.058
IPI2	0.027	**0.811**	0.118	0.069	0.224	0.045	0.121	0.054	-0.045	0.19
IPI3	0.16	**0.767**	0.203	0.217	0.209	-0.026	0.172	0.066	-0.029	0.038
IPI4	0.106	**0.68**	0.188	0.07	0.213	-0.09	0.137	0.07	0.03	0.122
PUE1	0.296	0.213	**0.869**	0.402	0.159	0.149	0.086	0.249	0.41	0.144
PUE2	0.341	0.103	**0.857**	0.413	0.084	0.07	0.052	0.219	0.443	0.09
PUE3	0.304	0.257	**0.707**	0.227	0.238	0.086	0.074	0.188	0.344	0.095
PTE1	0.354	0.184	0.244	**0.731**	0.229	0.024	0.258	0.208	0.198	-0.142
PTE2	0.375	0.22	0.343	**0.797**	0.184	0.1	0.053	0.169	0.309	-0.042
PTE3	0.549	0.082	0.372	**0.804**	0.124	0.087	-0.001	0.202	0.395	0.049
PTE4	0.445	0.152	0.409	**0.822**	0.207	0.169	0.142	0.239	0.386	0.085
PSA1	0.049	0.292	0.175	0.176	**0.891**	0.005	0.337	0.321	0.139	0.29
PSA2	0.087	0.228	0.166	0.226	**0.891**	0.048	0.361	0.311	0.067	0.224
PSA3	0.091	0.228	0.162	0.22	**0.862**	-0.031	0.262	0.262	0.169	0.221
PRT1	0.07	0.016	0.045	0.067	-0.01	**0.79**	-0.065	-0.152	-0.041	0.13
PRT2	0.095	0.008	0.208	0.141	0.05	**0.732**	0.093	0.029	0.092	0.039
PRT3	0.052	-0.07	0.053	0.086	-0.016	**0.803**	-0.164	-0.063	-0.05	0.049
TRG1	-0.071	0.215	-0.036	0.091	0.274	-0.068	**0.789**	0.203	-0.04	0.035
TRG2	0.034	0.068	0.178	0.152	0.288	-0.097	**0.76**	0.3	0.05	-0.039
TRG3	-0.001	0.113	0.066	0.085	0.273	0.016	**0.753**	0.193	-0.025	0.081
DPT1	0.07	0.02	0.207	0.157	0.23	-0.117	0.236	**0.865**	0.27	0.061
DPT2	0.134	0.128	0.164	0.171	0.338	-0.07	0.314	**0.815**	0.1	-0.004
DPT3	0.168	0.011	0.298	0.321	0.271	-0.011	0.188	**0.79**	0.249	0.002
SQE1*	0.305	0.014	0.443	0.332	0.191	-0.031	0.006	0.273	**0.818**	-0.027
SQE2*	0.154	0.14	0.332	0.331	0.2	0.106	0.121	0.19	**0.456**	0.024
SQE3*	0.28	-0.042	0.236	0.209	-0.076	-0.036	-0.098	0.056	**0.692**	-0.057
EXI1	-0.03	0.149	0.077	-0.056	0.312	0.006	0.032	0.007	-0.041	**0.827**
EXI2	0.019	0.077	0.134	0.031	0.144	0.076	0.002	0.068	-0.002	**0.759**
EXI3	0.055	0.047	0.095	0.01	0.137	0.156	0.046	-0.029	-0.044	**0.598**

* Formative Indicator.

** Emergent Construct.

In addition, there were several perceivable terrorist threats between the official end of the war and our second survey (e.g., the roll back of DHS' terrorism threat level to "high" in December 2003, followed by international flight cancellations and delays caused by terrorism intelligence). From these situations, we assume that the extended period of the external threat hampered the deduction of perceived risk and trust in the US government.

The new variable, DpTxExI, is a construct designed to measure the interaction effect of disposition to trust (DpT) and experience with the Internet (ExI) on perceived structural assurance of the Internet (PSA). To measure the interaction effect, we followed the product indicators technique suggested by Chin *et al*. [57]. According to their study, this technique has a superior detection power and accuracy in comparison to the summated regression technique. This technique was also appropriate to our study as we already adopted PLS to test our structural model, and the additional interaction variable allows us to jointly examine the potential direct effect and interaction effect of the moderating variable at the same time. The standardized values of the three DpT and three ExI indicators were extracted from the PLS measurement model's data matrix and multiplied in MS Excel, resulting in 9 product indicators for DpTxExI.

The structured model was first tested with combined data (*n*= 269) to detect relationships general to different times, situations, and e-Government agency characteristics. Then, the data were divided into two groups; anti/counter-terrorism (ACT) and non-ACT e-Government services, in order to examine relationships influenced by service domain and agency characteristics. ACT group includes FBI (*n=103*) and NYSOPS (*n=54*) data, and the non-ACT dataset consists of NYDMV data (*n=112*). The results from these analyses are presented in the next section.

Table 7. Mean Difference in Exogenous Variables

	2003	2004	Mean Difference	t stat.
PRT	0.027	-0.038	0.065	0.521
TrG	0.203	-0.276	0.479	3.931**
DpT	0.032	-0.045	0.077	0.619
SQE	-0.067	0.096	-0.163	-1.312
ExI	0.037	-0.054	0.091	0.733

* *p* < .05, ** *p* < .01, *** *p* < .001.

Results

Pooled Model – Direct Determinants

The graphical results of structured model analyses are presented in Figures 2, 3, and 4. The combined data model shows that many relationships found in the private-sector IT/e-commerce acceptance studies also hold in the e-Government context, but some noticeable discrepancies also exist. First, the R^2 of intention to provide personal information (IPI) was much lower than the R^2 of intention to depend on information (IDI). About 34 percent of variance in IDI was explained by perceived usefulness of the e-Gov website (PUE) (*β*= .179, p< .01), perceived trustworthiness of the e-Gov website (PTE) (*β*= .495, p< .01), and perceived structural assurance in the Internet (PSA) (*β*= -.056, ns). In contrast, the R^2 for IPI was only 12 percent. The effect of PTE, which was very strong on IDI, was not significant on IPI (*β*= .082, ns). Instead, PSA became the strongest predictor (*β*= .234, p< .01), followed by PUE (*β*= .155, p< .01).

With regard to the inter-relationship between PTE, PUE, and PSA, positive effect of PUE on PTE was statistically and substantively significant (*β*= .254, p< .01), while the effect of PSA was not (*β*= .081, p> .05).

Pooled Model – Indirect Determinants

A perceived risk of terrorism (PRT) was found to have a significant and positive effect (*β*= .132, p< .05) on perceived usefulness of e-Government websites (PUE). Also, the positive effect of trust in supreme government (TrG) on perceived structural assurance of the Internet (PSA) was found to be significant (*β*= .263, p< .01). However, the hypothesized positive relationship between TrG and PTE was not supported (*β*= .044, ns).

The system quality of an e-Government website (SQE) showed a very strong positive effect on PUE (*β*= .501, p< .01) and a strong positive effect (*β*= .277, p< .01) on PTE. Another control variable, disposition to trust (DpT) had strong positive effects on both trust in the supreme government (TrG) (*β*= .311, p< .01) and the structural assurance (PSA) (*β*= .259, p< .01), but not on the trust in e-Government websites (PTE) (*β*= .078, ns). In addition to DpT, experience with the Internet (ExI) (*β*= .277, p< .01) and the interaction of the two variables (DpTxExI) (*β*= .146, p< .01) had significant positive effects on the structural assurance (PSA).

ACT Model

In the next step, we analyzed only the data from anti/counter-terrorism e-Government services (ACT) (i.e., NYSOPS and FBI) in order to capture idiosyncratic characteristics of the particular service class. The ACT model showed a relationship pattern similar to the pooled model. Perceived Trustworthiness of an e-Government website (PTE) is again the strongest determinant (*β*= .564, p< .01) of the dependency intention (IDI), followed by the usefulness perception (PUE) (*β*= .187, p< .01). Interestingly, the negative non-significant effect of structural assurance perception (PSA) in the pooled model became more substantive and statistically significant (*β*= -.143, p< .05).

For the intention to provide personal information (IPI), PSA was the only significant determinant (*β*= .234, p< .05). PUE had a larger path coefficient (*β*= .167, ns) than the pooled model, but statistically non-significant. The variances explained for IDI and IPI were about 44 percent and 8 percent respectively, showing a lack of explanatory power of e-commerce determinants for online e-Government transactions. The effect of PUE on PTE was again strong and significant (*β*= .342, p< .01), while that of PSA on PTE was not (*β*= .054, ns).

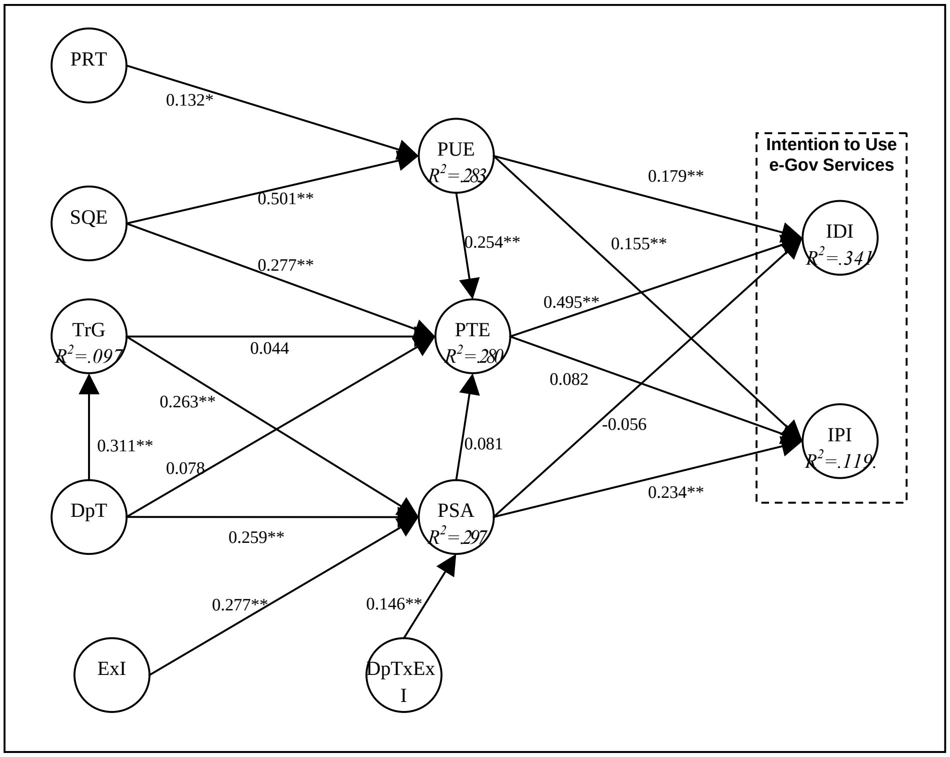

Figure 2. Effects of Risk and Trust on e-Gov Usage Intention (NYSOPS, FBI, and DMV)

In terms of the effects of perceived risk of terrorism (PRT) and trust in the government (TrG), ACT model showed the same effects on the direct determinants as in the pooled model. PRT had a significant positive relationship with PUE (β= .179, p< .05). TRG had a significant and positive effect on PSA (β= .276, p< .01), but not on PTE (β= .062, ns) again. System quality (SQE) had a strong positive effect on PUE (β= .412, p< .01) and PTE (β= .281, p< .01), as disposition to trust (DpT) had on TrG (β= .252, p< .01) and PSA (β= .240, p< .01). Experience with the Internet (ExI) also significantly influenced PSA (β= .364, p< .01), but the interaction effect (DpTxExI) became non-significant (β= .157, ns), in spite of the larger path coefficient than the pooled model.

Non-ACT Model

The relationship pattern found in NYDMV service data revealed striking deviation from the ACT model. Most of all, the positive effects of perceived usefulness (PUE) (β= .155, ns) and the structural assurance belief (PSA) (β= .049, ns) on intention to depend on information (IDI) became statistically non-significant, resulting in much less variance explained (R^2= .266) than in the ACT model. On the other hand, the effect of perceived trustworthiness of the e-Government website (PTE) on intention to provide personal information (IPI) (β= .293, p< .01) greatly increased and explained a larger portion of the variance in IPI (R^2= .245), compared to the ACT model. The inter-relationships between the direct determinants (i.e., PUE, PTE, PSA) were statistically not supported. The effect of perceived risk of terrorism (PRT) on PUE was positive, but not statistically significant (β= .118, ns). The direct effect of experience with the Internet (ExI) (β= .175, p< .05) and its interaction effect with DpT (β= .207, p< .05) on PSA were both positive and significant. Other control variables (i.e., SQE and DpT) showed the same effects as in the other two models. Table 8 summarizes the results of hypotheses testing.

An important finding from the analysis is the inconsistency of the relationships in different e-Government service categories.

Although the relationship pattern in the pooled model generally confirms previous findings in the private sector, the disaggregated models reveal the idiosyncrasy of each service class and the lack of explanatory power of the traditional information system acceptance models. The most distinguishable difference is that the magnitude of the effects of perceived usefulness (PUE), perceived trustworthiness (PTE), and perceived structural assurance (PSA) change significantly depending on the domain and the type of e-Government

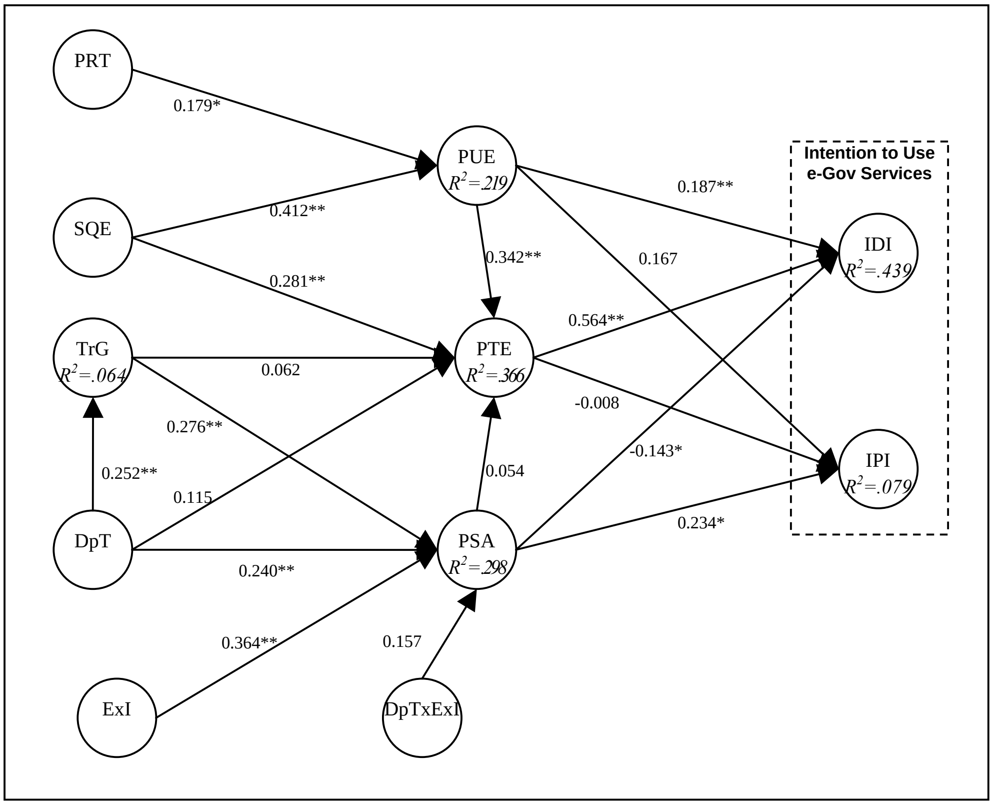

Figure 3. Effects of Risk and Trust on e-Gov Usage Intention (NYSOPS and FBI)

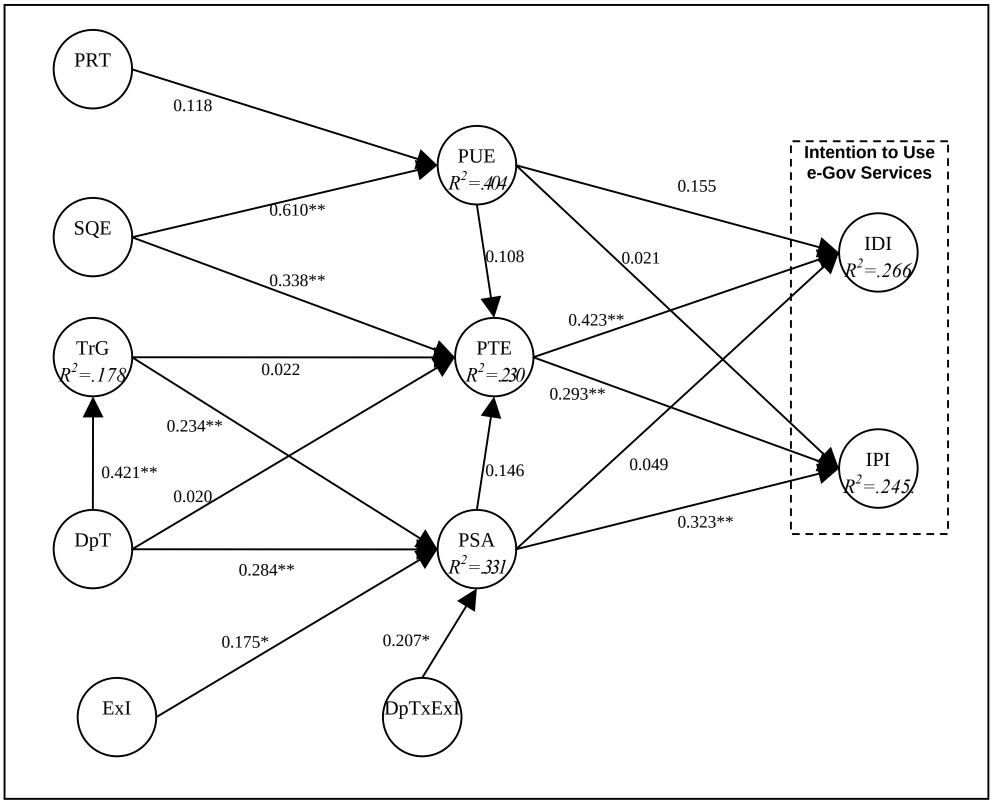

Figure 4. Effects of Risk and Trust on e-Gov Usage Intention (NYDMV)

services. That is, PTE has a strong positive effect on IDI, but not on IPI for ACT service category, while it exerts strong positive effects on both IDI and IPI for non-ACT services. Also, PSA shows a negative effect on IDI in ACT cases, but not in the non-ACT cases. Yet, PSA demonstrates a consistent positive effect on IPI for both models. Another important finding is that perceived risk of terrorism (PRT) significantly affects PUE only for ACT services, although its positive effect exists in non-ACT services. Trust in supreme government (TrG) positively and significantly affects PSA, and the effect is consistent across service categories. Finally, the positive sign of the interaction variable DpTxExI suggests that the effect of Internet experience (ExI) on PSA requires a supplementary relationship with disposition to trust (DpT) rather than a complementary relationship.

Table 8. Summary of Hypotheses Testing

Hypotheses	Pooled Model	ACT Model	Non-ACT Model
H1a. PUE →IDI (+)	Supported	Supported	Not supported
H1b. PUE → IPI (+)	Supported	Not supported	Not supported
H1c. PUE → PTE (+)	Supported	Supported	Not supported
H2a. PTE → IDI (+)	Supported	Supported	Supported
H2b. PTE → IPI (+)	Not supported	Not supported	Supported
H3a. PSA → IDI (+)	Not supported	Opposite Direction	Not supported
H3b. PSA → IPI (+)	Supported	Supported	Supported
H3c. PSA → PTE (+)	Not supported	Not supported	Not supported
H4. PRT → PUE (+)	Supported	Supported	Not supported
H5a. TrG → PTE (+)	Not supported	Not supported	Not supported
H5b. TrG → PSA (+)	Supported	Supported	Supported
H6a. SQE → PUE (+)	Supported	Supported	Supported
H6b. SQE → PTE (+)	Supported	Supported	Supported
H7a. DpT → TrG (+)	Supported	Supported	Supported
H7b. DpT → PSA (+)	Supported	Supported	Supported
H7b. DpT → PTE (+)	Not supported	Not supported	Not supported
H8a. ExI → PSA (+)	Supported	Supported	Supported
H8b. DpTxExI → PSA (-)	Opposite Direction	Not supported	Supported

Discussions

This study integrated various theories of IS acceptance previously developed in the private sector, and the model was extended in the e-Government context to explore the effect of terrorism risk and trust in government on citizens' e-Government usage intentions. Citizens' perceptions and usage intentions on two classes of e-Government websites, ACT and non-ACT service websites, were analyzed as a whole, as well as disaggregated groups. The results are very interesting. Most of all, the result suggests that external threats affect citizens' use of e-Government website in two ways. First, perceived risk of terrorism significantly increases perceived usefulness of anti/counter-terrorism e-Government. This relationship is evident, but not significant in non-ACT cases. It seems that when an external threat is realized, people perceive e-Government services that are directly related to the threat to be more useful, and are inclined to depend on the information provided by those e-Government websites. Second, trust in supreme government, which had dropped significantly over the research period, has considerable impact on perceived structural assurance of the Internet. When TrG decreases, citizens' belief in the safety of the Internet infrastructure also decreases, which in turn will impair citizen-to-government information transactions through e-Government websites.

For anti/counter-terrorism services, perceived trustworthiness of the e-Government website is the most critical determinant of citizens' intention to depend on the information. Perceived usefulness of the website is also an important factor, but its effect is largely mediated by PTE. Both PUE and PTE are strongly influenced by the system quality of the website. Our SQE measure includes organization, interactivity, loading speed, and feedback mechanism of a website. Therefore, e-Government initiatives need to improve those dimensions of their system quality in order to improve citizens' PUE and PTE, which will lead to higher intention to use the websites. Also, finding additional dimensions and developing more specific measure of system quality will be a meaningful study.

The contradicting negative relationship between perceived structural assurance in the Internet and IDI is significant for the ACT model, and it seems real. This may be explained by service substitutability, or information availability. IDI for ACT services are usually terrorism related news, directions, advice, etc.. Such information can be acquired not only from e-Government websites but also from non-government websites (e.g., news networks, terrorism research NGOs). When the Internet is technically and legally robust and reliable, there is no reason for citizens to depend on a single source of information. In fact, a citizen poll [49] shows that 56 percent of American Internet users went to online websites immediately before and after the break out of the Iraq war, and the most important reason for that was to get news from a variety of sources (66 percent), followed by timeliness of the information (63 percent). Supporting this, US government sites were the third most frequently visited sites, following American TV network (32 percent) and newspaper (29 percent) sites. Citizens also referred to foreign news organizations (10 percent). Disappearance of this negative effect in non-ACT services may also result from information availability. Even if non-government websites are equally reliable, there are not many websites that can provide as comprehensive and accurate information about automobile/traffic regulations as DMVs. Therefore, it is expected that only when a government agency is the original and the only source of information, structural assurance of the Internet can increase citizens' reliance intention on the information provided by the website.

With regard to citizens' intention to provide personal information, the only significant determinant in our ACT model was perceived structural assurance of the Internet, which resulted in a very low explanatory power ($R^2 < .08$). This shows a clear contrast to the non-ACT model that perceived trustworthiness in e-Government website exerts a significant effect (β= .293, p< .01), explaining about 25 percent of IPI, together with PSA (β= .323, p< .01). Moreover, additional t-test and ANOVA revealed that the mean value of IPI in ACT service category is significantly lower than that in non-ACT services.[18] When it is considered that most ACT services require citizens to provide personal information when they report terrorism-related information, we can predict that the current ACT e-Government websites fall short in its capability, and yet we do not know how to remedy this problem. Therefore, what causes the low intention of citizens to provide personal information to ACT class e-Government websites is left as an important and urgent topic of future research. Until we find additional determinants of IPI, we may

[18] Tukey, Scheffe, and Bonferroni Post-Hoc tests all showed significant mean difference between Non-ACT (i.e., NYDMV) and ACT (i.e., NYSOPS and FBI) services at p<.05. The difference between ACT-State (i.e., NYSOPS) and ACT-Federal (i.e., FBI) was not significant at the same significance level. IDI values of the two (ACT vs. non-ACT) and three (non-ACT State vs. ACT-State vs. ACT-Federal) groups were statistically identical.

need to improve citizens' perception on Internet safety, which can be achieved through increasing citizens' trust in the supreme (i.e., federal) government and increased use and experience of the Internet in general.

Another noticeable result is that trust in supreme government does not have a significant effect on perceived trustworthiness of a specific e-Government website. The path coefficients were negligible across the different e-Government categories (β= .062, ns for ACT; β= .022, ns for non-ACT). Therefore, we can conclude that, at least in the US government organization, trust in the supreme government is not inherited to its e-Government agencies in the organizational hierarchy. This means that even if citizens highly trust the supreme government, e-Government websites may not be able to benefit from its membership in the government organizations, and must build their own trustworthiness. As mentioned above, improving system quality of their website is one way to do so.

In sum, the findings of this study revealed the stark difference between different domains and types of e-Government services. As a consequence, the models and determinants from previous IS acceptance theories are limited in their applicability and explanatory power in the context of e-Government. The results of our analysis provide valuable information about the idiosyncratic characteristics and important factors in e-Government acceptance models, which can be used for further development of theories and measurement instruments that can better fit the e-Government context. We hope that our results provide many e-Government and public safety researchers with useful empirical evidence and rich insight on how external threats influence citizens' intention to use e-Government services. Government, with these findings, will also be able to secure stable functioning of its online operations and improve services, especially in the presence of an external threat.

References

1. e-Gov. E-Gov and IT Accomplishments. Electronic Document <http://www.whitehouse.gov> 2003.
2. e-Gov. E-Gov Initiatives at a Glance. Electronic Document <http://www.whitehouse.gov/omb/egov/downloads/E-Gov_Initiatives.pdf> 2004.
3. OMB. FY 2003 Report to Congress on Implementation of The E-Government Act. Electronic Document <http://www.whitehouse.gov/omb/egov/fy03_egov_rpt_to_congress.pdf> 2004.
4. Gant, D. B., J. P. Gant and C. L. Johnson. State Web Portals: Delivering and Financing E-Service. The PricewaterhouseCoopers Endowment for the Business of Government, 2002.
5. PewInternet. "Pew Internet Project Data Memo." Pew Internet & American Life Project. Electronic Document <www.pewinternet.org.> 2003.
6. Wulf, W. A., Y. Y. Haimes and T. A. Longstaff. "Strategic Alternative Responses to Risk of Terrorism." Risk Analysis. 23:3. 2003: 429-44.
7. CEG. E-Government: The Next American Revolution. The Council for Excellence in Government, 2001.
8. PewInternet. "Counting on the Internet." Pew Internet & American Life Project. 2002.
9. PewInternet. "The Internet and the Iraq War." Pew Internet & American Life Project. Electronic Document <www.pewinternet.org.> 2003.
10. Baker, J. C., et al. Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information. (Ed.) N. D. R. Institute. RAND Corporation, 2004.
11. Sparks, P. and R. Shepherd. "Public Perceptions of Food-related Hazards: Individual and Social Dimensions." Food Quality and Preference. 5:3.1994: 185-94.
12. Tiwana, A. and A. Bush. "A Social Exchange Architecture for Distributed Web Communities." Journal of Knowledge Management. 5:3. 2001: 242-8.
13. Doll, W. J., et al. "A Confirmatory Factor-Analysis of the User Information Satisfaction Instrument." Information Systems Research. 6:2. 1995: 177-88.
14. Bharadwaj, A. S. "A Resource-based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation." MIS Quarterly. 24:1. 2000: 169-96.
15. Gupta, A., B.-C. Su and Z. Walter. Economic Analysis of Consumer Purchase Intentions in Electronic and Traditional Retail Channels: Competitive and Strategic Implications. Decision Support Systems, 2003.
16. Venkatesh, V., et al. "User Acceptance of Information Technology: Toward a Unified View."MIS Quarterly. 27:3. 2003: 425-78.
17. Davis, F. D. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." MIS Quarterly. 13:3. 1989: 319-40.
18. McKnight, D. H., L. L. Cummings and N. L. Chervany. "Initial Trust Formation in New Organizational Relationships." The Academy of Management Review. Academy of Management. 23:3. 1998: 473-90.
19. McKnight, D. H., V. Choudhury and C. Kacmar. "Developing and Validating Trust Measures for E-commerce: An Integrative Typology." Information Systems Research. 13:3. 2002: 334-59.

20. Davis, F. D., R. P. Bagozzi and P. R. Warshaw. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models." Management Science. 35:8. 1989: 982-1003.

21. Fishbein, M. and I. Ajzen. Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. Reading: Addison-Wesley, 1975.

22. Azjen, I. and M. Fishbein. Understanding Attitudes and Predicting Social Behavior. Englewood Cliffs: Prentice-Hall, Inc., 1980.

23. Venkatesh, V. and M.G. Morris. "Why Don't Men Ever Stop to Ask for Directions?: Gender, Social Influence, and Their Role in Technology Acceptance and Usage Behavior." MIS Quarterly. 24:1. 2000: 115-39.

24. Szajna, B. "Empirical Evaluation of the Revised Technology Acceptance Model." Management Science. 42:1. 1996: 85-92.

25. Venkatesh, V. and F. D. Davis. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies." Management Science. 46:2. 2000: 186-204.

26. Hartwick, J. and H. Barki. "Explaining the Role of User Participation in Information System Use." Management Science. 40. 1994: 4.

27. Thompson, R. L., C. A. Higgins and J. M. Howell. "Personal Computing: Toward a Conceptual Model of Utilization." MIS Quarterly. 15:1. March 1991: 125-42.

28. Moore, G. C. and I. Benbasat. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation." Information Systems Research. 2:3. 1991: 192-222.

29. Premkumar, G., K. Ramamurthy, and S. Nilakanta. "Implementation of Electronic Data Interchange: An Innovation Diffusion Perspective." Journal of Management Information Systems. 11:2. 1994: 157-86.

30. Davis, F. D., R. P. Bagozzi and P. R. Warshaw. "Extrinsic and Intrinsic Motivation to Use Computers in the Workplace." Journal of Applied Social Psychology. 22:14. 1992: 1111-32.

31. Compeau, D. R. and C. A. Higgins. "Computer Self-Efficacy: Development of a Measure and Initial Test." MIS Quarterly. 19:2. 1995: 189-211.

32. Gefen, D., E. Karahanna, and D. Straub. "Trust and TAM in Online Shopping: An integrated Model." MIS Quarterly. 27:1. 2003: 51-90.

33. Waldman, S. R. Foundation of Political Action: An Exchange Theory of Politics. Boston: Little Brown, 1972.

34. Baldwin, D. A. "Power and Social Exchange." The American Political Science Review. 71:4. 1978: 1229-42.

35. Kim, D. J., et al. A Multi-dimensional Trust Formation Model in B-to-C E-Commerce: A Conceptual Framework and Content Analysis of Academia/Practitioner Perspectives. Decision Support Systems, Forthcoming.

36. Mayer, R. C., J. H. Davis and F. D. Schoorman. "An Integration Model of Organizational Trust." Academy of Management Review. 20:3. 1995: 709-34.

37. Bhattacherjee, A. "Individual Trust in Online Firms: Scale Development and Initial Test." Journal of Management Information Systems. 19:1. 2002: 211-41.

38. PewInternet. "How Americans Used the Internet after the Terror Attack." Pew Internet & American Life Project. 2001.

39. Kreps, D. M. A Course in Microeconomic Theory. Princeton, NJ: Princeton University Press, 1990.

40. Savage, L. J. The Foundations of Statistics. New York: Wiley, 1954.

41. Ellsberg, D. "Risk, Ambiguity, and the Savage Axioms." Quarterly Journal of Economics. 75. 1961: 643-69.

42. Curley, S. P., J. F. Yates and R. A. Abrams. "Psychological Sources of Ambiguity Avoidance." Organizational Behavior and Human Decision Processes. 38:2. 1986: 230-56.

43. Curley, S. P. and J. F. Yates. "The Center and Range of the Probability Interval as Factors Affecting Ambiguity Preferences." Organizational Behavior and Human Decision Processes. 36:2. 1985: 273-87.

44. Casey, J. T. and J. T. Scholz. "Boundary Effects of Vague Risk Information on Taxpayer Decisions." Organizational Behavior and Human Decision Processes. 50:2. 1991: 360-94.

45. Blau, P. M. Exchange and Power in Social Life. Transaction Pub, 1986.

46. Gefen, D. "E-commerce: The Role of Familiarity and Trust." The International Journal of Management Science. 28:6. 2000: 725-37.

47. Luhman, N. Trust and Power. Chichester: Wiley, 1979.

48. Cook, T. D. and D. T. Campbell. Quasi-Experimentation: Design and Analysis Issues for Field Settings. Boston: Houghton Mifflin Company, 1979.

49. PIP. "The Internet and the Iraq War: How Online Americans Have Used the Internet to Learn War News, Understand Events and Promote Their Views." Pew Internet & American Life Project. 2003.

50. Gordon, M. E., L. A. Slade and N. Schmitt. "The 'Science of the Sophomore' Revisited: From Conjecture to Empiricism." Academy of Management Review. 11:1. 1986: 191-207.

51. E-Gov. E-Gov and IT Accomplishments. E-Gov, 2003.

52. Kim, J., et al. "Businesses as Buildings: Metrics for the Architectural Quality of Internet Businesses." Information Systems Research. 13:3. 2002: 239-54.

53. Palmer, J. W. "Web Site Usability, Design, and Performance Metrics." Information Systems Research. 13:2. 2002: 151-67.

54. Barclay, D., C. Higgins and R. Thompson. "The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration." Technology Studies. 2:2. 1995: 285-324.

55. Chin, W. W. "The Partial Least Squares Approach for Structural Equation Modeling" Modern Methods for Business Research. (Ed.) G. A. Marcoulides. Lawrence Erlbaum Associates, 1998. 295-336.

56. Hair, J. F., Jr., et al. Multivariate Data Analysis with Readings. 4th Edition. Englewood Cliffs: Prentice Hall, 1995.

57. Chin, W. W., B. L. Marcolin and P. R. Newsted. "A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion / Adoption Study." Information Systems Research. 14:2. 2003: 189.