Available online at www.sciencedirect.com
ScienceDirect
Journal of Strategic Information Systems 17 (2008) 214–233
Strategic Information Systems
www.elsevier.com/locate/jsis

Internet privacy concerns and beliefs about government surveillance – An empirical investigation

Tamara Dinev [a,*], Paul Hart [a], Michael R. Mullen [b]

[a] Department of Information Technology and Operations Management, Barry Kaye College of Business, Florida Atlantic University, Boca Raton, FL 33431, USA
[b] Department of Marketing, Barry Kaye College of Business, Florida Atlantic University, Boca Raton, FL 33431, USA

Received 16 January 2006; accepted 11 September 2007
Available online 19 November 2007

Abstract

This U.S.-based research attempts to understand the relationships between users' perceptions about Internet privacy concerns, the need for government surveillance, government intrusion concerns, and the willingness to disclose personal information required to complete online transactions. We test a theoretical model based on a privacy calculus framework and Asymmetric Information Theory using data collected from 422 respondents. Using LISREL, we found that privacy concerns have an important influence on the willingness to disclose personal information required to transact online. The perceived need for government surveillance was negatively related to privacy concerns and positively related to willingness to disclose personal information. On the other hand, concerns about government intrusion were positively related to privacy concerns. The theoretical framework of our study can be applied across other countries.

Keywords: E-commerce; Privacy; Government; Surveillance; LISREL

1. Introduction

Sociologists have argued that the current American society is a surveillance society (Lyon, 2001; Norris and Armstrong, 1999; Stadler, 2002). Surveillance refers to any collection and processing of personal data, whether identifiable or not, for purposes of influencing or managing those whose data have been garnered (Lyon, 2001, p. 2). Both private corporations and government agencies take advantage of the increasing technical capability of information systems to collect and process consumer and citizen data. They use this vast amount of data to build profiles to acquire knowledge about consumer preferences for commercial purposes and citizen behaviors to detect and prevent security breaches, fraud and other crimes, and terrorist activities.

This study focuses on Internet users' responses to government initiatives intended to address the above mentioned threats to society. The international diffusion of the Internet has provided many social benefits

* Corresponding author. Tel.: +1 561 297 3181.
E-mail addresses: tdinev@fau.edu (T. Dinev), hart@fau.edu (P. Hart), mullen@fau.edu (M.R. Mullen).

0963-8687/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.jsis.2007.09.002

but at the same time the Internet provides an online venue for opportunistic and malicious activity. Thus, numerous sources of crime and security threats have emerged online. The possibility of terrorist threats led Clarke (2001) to warn of the dangers of digital sabotage intended to disrupt and damage the economy. Professional and organized cybercrime targeting financial institutions and the e-commerce infrastructure grew 35 times over during the last 4 years (Grow, 2005). Cybercrime (i.e., virus attacks, network break-ins, online scams) has been identified as the U.S. Federal Bureau of Investigation's (FBI) third highest priority, after counter-terrorism and counter-intelligence (Grow, 2005). The FBI's cybercrime strategy created in 2002 includes extensive Internet surveillance and intelligence gathering at both vendor and online service provider levels (Grow, 2005). Clearly, there has been less public tolerance for security compromises and crimes since September 11th(Kary, 2002). Thus, the nature and the seriousness of the security threats would seem to make surveillance a welcome and justifiable practice and the subjects – voluntary participants (Lyon, 2001).

However, at the same time, American legal precedent and public opinion reflect a society in which privacy is highly valued (Laufer and Wolfe, 1977; Rosen, 2001). Americans view privacy as an expression and safeguard of personal dignity (Cohen, 2000; Swire, 1999, 2003). Privacy is among the highest of individual rights (Etzioni, 1999; Westin, 1967, 2001). When asked what Americans feared the most in the upcoming century, a 1999 Wall Street Journal poll found that 29% of the respondents ranked erosion of personal privacy first among a list of more frightening concerns including world war, global warming, and international terrorism, none of which was ranked first by more than 23% of the respondents (Harvey, 1999). In Congressional testimony to the House Subcommittee on Commerce, Trade, and Consumer Protection, Westin (2001) summarized the results of a series of polls conducted in collaboration with Louis Harris and Associates and Equifax throughout the 1990s. In one poll, 79% of the respondents believed that if the Framers of the Declaration of Independence were rewriting that document today, they would add privacy to the trinity of life, liberty, and pursuit of happiness (p.11). In another, a majority ranked privacy just behind freedom of speech and ahead of freedom of religion and the right to vote as the most important American right (p. 11). And in still another poll, 94% said they are worried about the potential misuse of their personal information, with 77% of those responding that they are very concerned (p. 11). The unmistakable belief in the right to privacy in American culture makes a recent observation by Rosen (2001) poignant and timely: in comparing British and American societies, Britain has embraced new surveillance technologies more readily, while America has strenuously resisted them.

Chapman (2000) observed that public concerns about privacy tend to exhibit cyclical patterns. Each cycle, of roughly 10 years, is triggered by events that catalyze public fears about losing privacy. At the beginning of each cycle, the erosion of privacy has been substantially consolidated and extended in depth and breadth as compared to the end of the previous cycle. The rapid development and prolific use of digital and Internet technologies and their capability for improving surveillance techniques explain the recent beginning of such a cycle of growing privacy concerns (Clarke, 1988; Marx, 2003). In commenting on this cycle over recent years, a number of social scientists have noted that greater privacy threats have been attributed to the private sector rather than the Orwellean prediction that placed big brother in the realm of the public sector (Laudon, 1997; Varian, 1997). This phenomenon has been referred to as the privacy paradox (Etzioni, 1999). Thus, the private sector, rather than the public sector, has been attributed with making consumers, as distinct from citizens, vulnerable (Marx, 2003; Noam, 1997).

The U.S. government has made some effort in the past to regulate to a certain extent the protection of personal information in the private sector, especially regarding health care. The Health Insurance Portability and Accountability Act (HIPAA) enacted by the U.S. Congress in 1996 contains the Privacy Rule establishing regulations for the use and disclosure of protected personal health information. Another notable effort in that direction is the Electronic Freedom of Information Act (FOIA) Amendments of 1996 that expand the scope of the original FOIA of 1966 to encompass electronic records and require the creation of electronic reading rooms to make federal agencies' records more easily and widely available to the public. The incorporated Privacy Act (PA) of 1974 further regulates the rights of an individual to gain access to information held by the government about oneself; the right to amend that information if it is inaccurate, irrelevant, untimely, or incomplete; and the right to sue the government for violations of the statute.

The events that have taken place since September 11th to fight terrorist threats appear to be shifting concerns about privacy vulnerability back to the public sector. In the U.S. alone, a number of initiatives based on the need to improve security to ensure social order have been undertaken. These include the Total Information

Awareness Program (Clymer, 2003); the Patriot Act of 2001, the Homeland Security Act of 2002, and a series of executive orders. Collectively, these initiatives give federal agencies greater authority to monitor individuals (Janofsky, 2002; Wald, 2004) and allow data sharing across agencies (Lichtblau, 2005) and between the private sector and federal agencies (Wald, 2004). Public opposition to this increased government surveillance has been substantially muted (Cha and Krim, 2001; Liptak, 2002). These initiatives have been an important catalyst for the growing debate about privacy among citizens of the U.S. (Toner and Lewis, 2001; Toner, 2001) and of the European countries (Hoge, 2001). The recent disclosure that the White House ordered the National Security Agency to conduct eavesdropping in the U.S. without warrants (Risen and Lichtblau, 2005; Sanger, 2005), significantly fueled concerns about privacy and the extent of government surveillance (Lichtblau and Share, 2006).

At the same time, given the possibility of increased cyber attacks, fraud, and further terrorist activity, the rapid evolution of the government initiatives to enhance surveillance has forced a debate about consolidating security and privacy (security and privacy) rather than agonizing between these two seemingly polar values (security vs. privacy) (Kling, 1996; Safire, 2004; Swire, 2001, 2003; Swire and Steinfeld, 2002; Rather, 2005).

We would further argue that in this new cycle of privacy concerns there is erosion in the perceived separateness of the two sources of privacy vulnerability – one based on the public sector and the other on the private sector (Campbell and Carlson, 2002). Networking technologies make the physical exchange of information gathering and analysis across both sectors more readily possible. And, policy initiatives, such as the Cyber-Security Enhancement Act (CSEA) of 2002, sanction the exchange of certain information collected in the private sector with the agencies in the public sector. CSEA allows government agencies to obtain e-mail, voice mail, phone records, and Web-based transactions, and other services from the private sector. Increased interest in personal information and behavior is also evident in the recent U.S. government subpoena of search data from Google and other search engine firms (Hafner and Richtel, 2006; Walker, 2006) – an initiative directed straight at the Internet user. Transactions conducted in cyberspace, in particular, generate detailed electronic footprints that expose individuals' preferences, interests, and behaviors. Thus, the Internet provides an unprecedented means to unobtrusively observe user Internet activity and to gather copious amounts of information about individuals and their transactions for both government and private sector purposes. For instance, it was recently reported that an anonymous individual AOL user was identified only from records of three months of search data (Barbaro and Zeller, 2006). Some privacy advocates refer to the unintended consequences of all that data being compiled, stored and cross-linked as a ticking privacy time bomb (Barbaro and Zeller, 2006) and argue that government subpoena of Internet users' search data will set a dangerous precedent that should worry all Americans (Elsner, 2006, p. D1).

These developments pose an important challenge which we address in this research. How do Internet users assess the need for greater surveillance to enhance security on the one hand and the need to ensure privacy to protect civil liberties on the other hand?

In the following section, we develop a theoretical framework for a model that considers privacy concerns and beliefs about government surveillance as antecedents to the willingness to provide personal information to transact on the Internet. We recognize that an individual's decision to actually provide private information over the Internet may well be influenced by many other factors such as personal interest (Dinev and Hart, 2006a), Internet literacy and social awareness (Dinev and Hart, 2006b), economic factors (saving time and or money), quality, and availability of relevant services and products. Additionally, classical Technology Acceptance Model (TAM) and Theory of Panned Behavior (TPB) factors and their influence in e-commerce use have also been extensively considered in the MIS literature (e.g. Pavlou and Fygenson, 2006, and most of Pavlou's research). The concept of privacy calculus (Culnan and Armstrong, 1999) has been introduced in the MIS literature, according to which a number of competing (positively and negatively influencing) factors might cause the individual to rise above their a priori intentions and/or concerns and anxieties, and actually provide the information in a given situation (Dinev and Hart, 2006a). Nonetheless, the objective of this study is to introduce and build the constructs of beliefs about government surveillance and examine their effects, along with privacy concerns, on the behavioral intention to provide the personal information, per se. Building a comprehensive model of all factors that influence user's decision to submit personal information online is beyond the scope of this study and a goal of future research.

The subsequent section describes the validation and assessment of the constructs within the nomological framework. In the final section, we discuss the results of our study and their implications. The findings suggest

that there is a dichotomy in attitudes among Internet users toward government initiatives intended to improve security. Both the perceived need for surveillance and concerns about government intrusion are evident resulting in a set of complex relationships between privacy concerns and willingness to disclose personal information over the Internet. The findings corroborate Westin's (2003) observation that: we are only beginning to observe … how the citizen-privacy issues presented by terrorism are changing prior segmentations. How the public will react to proposals for in-depth government monitoring of consumer transactions and communications, in the search for terrorists, will be increasingly the focus of privacy debates in this decade.

2. Theoretical framework

While scholars from a range of disciplines, including human resources (e.g., Stone and Stone, 1990; Tolchinsky et al., 1981) and social psychology (e.g., Kelvin, 1973), have addressed privacy issues, MIS researchers' interests in privacy (Mason, 1986) have paralleled the development of digital network and storage technologies. Important research in the discipline has focused on a range of issues including: managers' responses to social expectations about developing corporate privacy policies (Smith, 1993), the influence of cultural values on national privacy regulation (Milberg et al., 1995, 2000) and corporate procedures for addressing employee privacy issues (Smith et al., 1996; Stone et al., 1983); developing measure of information privacy concerns (Smith et al., 1996; Stewart and Segars, 2002); the importance of allowing individuals control over how personal information collected by corporations should be used (Culnan, 1993; Milne, 2000; Phelps et al., 2000); assessments of how well public and private organizations comply with self-regulatory expectations to ensure privacy (Culnan, 2000; Milberg et al., 2000; Milne and Culnan, 2002); and, the importance of privacy in online transactions (Culnan and Armstrong, 1999; Dinev and Hart, 2006a). This research falls within the last category (online transactions) and focuses on privacy concerns, their relationship to perceived needs to increase government surveillance, concerns about government intrusion and the willingness to disclose personal information to complete transactions on the Internet.

Sociologists have linked modernity with the tendency of public and private bureaucracies to increase control and power (Beniger, 1986; Giddens, 1985), and surveillance is the perfect tool to accomplish that (Gilliom, 2001). Lyon (1994, 2001) has written extensively about surveillance. Lyon reasons that the increasingly routine, systematic and focused attention paid by organizations to individual's lives – hence 'surveillance' – [i]s part of an overarching process (2001, p. 109) that is consistent with classic conceptions of modernity. Justifications for surveillance by government agencies and economic institutions are based on the need to maintain social order and economic management. Lyon (1994) has further argued if it were ever useful to separate 'public' and 'private' spheres for analytical purposes, it certainly is not … in late twentieth century, when the boundaries between them have been thoroughly obscured (p. 16). Information technology plays a central role in increasingly blurring these boundaries. When the home, which was once a haven from 'public' life is increasingly, the site of surveillance (Lyon, 1994, p. 16) privacy is less certain but at the same time highly valued.

The nature of surveillance constitutes an asymmetric or imperfect information situation in which one party has more or better information than the other (Akerlof, 1970). The well-known description of Bentham's plan for a penitentiary in the late 18th century called the Panopticon, or all seeing place is an example of an asymmetric arrangement in a closed environment. Following the plan, the subjects could always be able to be seen but not know whether they were seen. In the open environment of markets, Laudon (1997) has argued that information asymmetries in the marketplace in general have increased as a result of the failure in the personal information market in particular. The failure is that the price of obtaining personal information is too low and does not reflect true social costs. This market failure has resulted in an exploitation of personal information gathering and processing by large organizations and in negative externalities, such as the loss of privacy for individuals.

The loss of privacy occurs when individuals are required to submit personal information to complete purchasing transactions. Many parties are involved in this process including Internet service providers, financial institutions, online marketers, and advertisers. However, other parties can be illegally or surreptitiously involved through spyware monitoring, keyboard logging, or hacking. Moreover, government-sponsored surveillance may also occur. All of these parties introduce information asymmetry. The imperfect knowledge of the buyer about how and by whom their personal information may be used, negatively affects the ability to

make informed transaction decisions (Noam, 1997). Moreover, negative consequences can occur at a much later time making it practically impossible to find the details required to know how and why the privacy violations occurred. The market failures related to the low price of gathering personal information have increased information asymmetries, which in turn affect further market failure by inhibiting consumer willingness to disclose personal information necessary to complete transactions (Laudon, 1997; Akerlof, 1977). The relatively lower cost of gathering and processing more personal information from Internet users implies that the potential for market failure is greater in the online environment compared to conventional transaction venues.

Scholars who study privacy have argued that an individual's intention to disclose personal information is based on a calculus of behavior or a decision process in which potentially competing factors are weighed in light of possible outcomes (Laufer and Wolfe, 1977; Stone and Stone, 1990). Culnan and Armstrong (1999) applied the notion of a privacy calculus to decisions made by consumers in the context of purchasing products and services (see also Culnan and Bies, 2003). They found that when businesses informed consumers about Fair Information Practices (FIP), consumers perceived them to be fair and were more willing to disclose personal information in purchasing transactions. Dinev and Hart (2006a) expanded the privacy calculus by investigating other factors and found that privacy risk and privacy concerns were negatively related to personal information disclosure in Internet transactions. However, these factors may be outweighed by trusting beliefs of consumer that personal information would be safeguarded and by their personal interest in obtaining the products, services, or information provided over the Internet.

The following theoretical model is based on the overall framework of a privacy calculus that accounts for information asymmetry and includes a set of contrary factors that are salient in the decision to disclose personal information in order to complete transactions on the Internet. The model is also based on the well-established framework for assessing information technology use in which a set of antecedent beliefs are assessed in relation to behavioral intentions (Davis, 1989; Venkatesh et al., 2003).

3. The theoretical model

To date, we are not aware of any empirical MIS research which has incorporated privacy concerns, beliefs about the need for government surveillance and at the same time concerns about government surveillance as antecedents to the behavioral intention to disclose personal information on the Internet. It is not clear how individuals intend to consolidate their potentially conflicting beliefs about the government's response to improve security and the potential threats to privacy, and how these beliefs will affect users' behavioral intentions in using the Internet. The dependent variable in the model described below is the willingness to provide the personal information required to complete transactions on the Internet (Dinev and Hart, 2006a). This construct refers to the intended use of the Internet in general rather than specific websites in particular. Because the focuses of our study are asymmetry of information and surveillance on the part of government and the influence these exert on attitudes – a certain online vendor or attributes of specific websites bear no relevance to the main research question. The theoretical model described below is summarized in Fig. 1 and each of the constructs is listed in Table 1.

3.1. Internet privacy concerns

Internet privacy concerns refer to perceptions about opportunistic behavior related to the disclosure of personal information submitted over the Internet (Dinev and Hart, 2006a). These concerns reflect the extent to which individuals believe they might lose their privacy. Privacy has been studied by researchers in a range of disciplines over many years (Margulis, 2003) although research on privacy and the Internet has only emerged in recent years. Privacy concerns are the single most cited reason for declining to use the Internet (Westin, 2001). According to a series of UCLA Reports (2000 through 2004), privacy and the requirement to submit personal information are the primary factors that discourage users from shopping online. Many consumers do not register at websites primarily because of privacy concerns and as many as 50% of consumers provide false information when asked to register at a website or respond to online surveys (BCG, 1998; Greenman, 1999). Malhotra et al. (2004) and Dinev and Hart (2004, 2006a) reported a positive relationship between Internet information privacy concerns and perceived risk in providing personal information over the Internet, and a

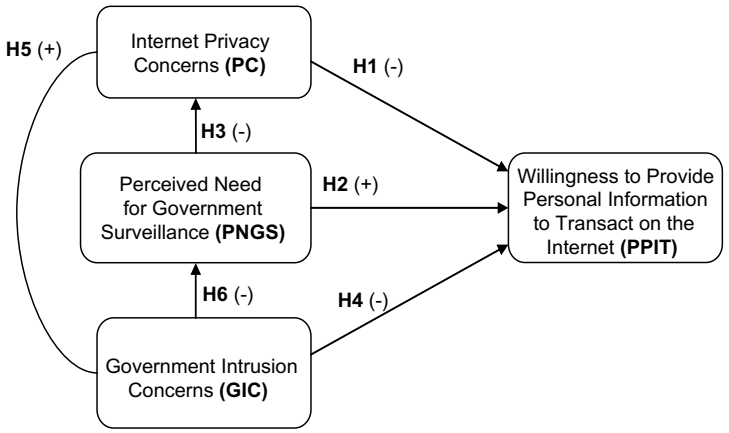

Fig. 1. Proposed theoretical model.

Table 1
Constructs in the study

Construct category	Construct	Acronym	Definition
Willingness to act	Willingness to provide personal information to transact on the Internet	PPIT	Willingness to provide personal information required to complete transactions on the Internet
Privacy and risk beliefs	Internet privacy concerns	PC	Concerns about opportunistic behavior related to the personal information submitted over the Internet by the respondent
	Government intrusion concerns	GIC	Concerns about government monitoring of user's Internet activity and account information
Confidence beliefs	Perceived need for government surveillance	PNGS	Perceived need for the government to have greater access to personal information and to monitor personal activities

negative relationship between perceived risk and intention to provide personal information (see also Dinev and Hart, 2006b). These findings suggest the following.

H(1). Internet privacy concerns are negatively related to the willingness to provide personal information to transact on the Internet.

3.2. Perceived need for government surveillance

The perceived need for government surveillance is the Internet users' belief that the government needs to increase security procedures and to ensure safe and reliable Internet transactions. More specifically, in our model, it is defined as the perception that the government needs greater access to personal information and greater authority to conduct surveillance of Internet transactions. This construct is intended to capture the perceived beneficial component of surveillance – Internet users welcome surveillance as a needed practice that will result in a variety of benefits such as security, social order, convenience, and ease. Because of these perceived benefits, Internet users may not only become voluntary participants (Lyon, 2001) but will tend to encourage surveillance practices.

The perceived need for government surveillance can be better understood if we derive it from risk (security). Sociologists (Starkey and McKinlay, 1998; Foucault, 1983) have identified risk as a critical dimension of the surveillance society, the other three being coordination, power, and privacy. Like all four dimensions which are also closely related to each other, mitigating risk is Janus-faced, that is, its characteristics have undeniable benefits but at the same time clearly involve constraints or costs (Flaherty, 1989; Lyon, 2001). Risk management has been extensively studied in MIS literature as also related to information security in organizations ((Rees et al., 2003; Straub and Welke, 1998; Dhillon and Backhouse, 2001) for a comprehensive review of information security research).

Risk involves the uncertainty and possibility of future peril. It is based on the perceived threats, or risks, to security in the environment including the Internet infrastructure. Institutions try to reduce risk and prevent potential threats by managing outcomes. Internet users who perceive the need for risk management also accept that the latter requires tracking of past events and activities with the intent to predict the future. Over the Internet, risk can come from two sources: unauthorized access to digitized information and threats to the infrastructure. Unauthorized access to information can be caused by any number of factors including accidental disclosure, insider curiosity, insider subordination, external hacking into computer systems, security defects, scams, and uncontrolled secondary usage of personal data (Rindfleish, 1997). Malicious attempts to disrupt online service through viruses and other programs have threatened to destroy computer systems and networks or impede authorized access to databases (Hu and Dinev, 2005) this causing harms to infrastructures. Our model does not attempt to assess the relative influence of specific sources of possible security risks discussed in the earlier sections of this paper. Rather, our model includes beliefs about government responses to security threats.

In this positive type of belief, individuals perceive that the information asymmetry related to possible illegal third parties is more disturbing than the asymmetry related to the possible presence of government surveillance. Thus, to protect themselves, individuals may feel that the government needs to be proactive in gathering and processing information about individuals in order to ensure a secure environment. Therefore, it is a positive belief that the government's gathering personal information online and monitoring online activities is for the purposes of protection, social order and reducing risk. Having this belief, Internet users do not feel inhibited to disclose personal information – the user accepts the possible surveillance of his or her personal information by the government. Moreover, they also feel encouraged to transact online, given the increased sense of safety and less risk. In a privacy calculus framework such as in Culnan and Armstrong (1999) or Dinev and Hart (2006a), perceived government surveillance would be mapped as the positive factor needed to ensure that personal information is not abused and online behavior is not compromised by unknown third parties with malicious intentions. We come to the conclusion argued by Swire (2003) that, to the extent that the surveillance initiatives ensure protection and reliability, they contribute to the fair information practices, which, in turn, are an important condition for the successful completion of online transactions.

H(2). Perceived need for government surveillance is positively related to the willingness to provide personal information to transact on the Internet.

Individuals who perceive the need for the government to be proactive will be less concerned that the government has access to their personal information (e.g., previous addresses, value of assets, etc.) and specific online behavior (see also Kling and Allen, 1996). The users assess their own privacy concerns and anxiety over personal risks from surveillance, and juxtapose them against society risks in general. Facing the need to compromise, the users would prefer that their own personal information be in the right hands of the government rather than in criminal hands and thus would be compliant with the need for information gathering. Indeed, the complexity of the relationship between privacy and risk can be seen in the paradox observed by Nock (1993) that the quest for privacy in the U.S. may actually give rise to surveillance (Lyon, 2001) supports this observation. Nock argues that surveillance is the necessary glue that ensures trust in a society of individuals who highly value privacy. As a society of members who barely know each other, citizens deny others access to their personal affairs (Lyon, 2001). Thus, in order to satisfy the need for businesses, institutions, and the government to trust us, they provide surveillance data about themselves (i.e., credentials such as driving licenses, credit card authorizations, third party confirmations, urine analysis results, and so on). Provided that the user feels that the government performs the surveillance in an ethical and appropriate manner (Marx, 1998), and with fair information practices in place (and that obviously would be the case if the user expresses a need for more government surveillance on the first place), privacy concerns will tend to decrease. These considerations suggest the following.

H(3). Perceived need for government surveillance is negatively related to Internet privacy concerns.

3.3. Government intrusion concerns

Concern about government intrusion is a negative belief about the proactive gathering and processing of personal information and monitoring online behavior by the government. In our model, government intrusion concerns are users' concerns about government monitoring of Internet activity and account information.

It is important to differentiate between privacy concerns and intrusion concerns. The latter can be present even if privacy is not perceived to be violated. The mere knowledge that one is being observed changes one's conscious behavior. For examples, even if the topic of conversation is not inherently private, opinions and actions become candidates for a third party's approval or contempt (Benn, 1982). Surveillance has social costs (Rosen, 2000) and inhibiting effects on spontaneity, creativity, productivity, and other psychological effects. Internet users will be reluctant to provide information for fear that their online activities may be monitored and the information gathered and processed becoming accessible to government agencies for subsequent scrutiny (Hafner, 2006; Safire, 2002). This asymmetric information arrangement can inhibit an individual's willingness to disclose information required to complete e-commerce transactions even if he or she does not believe that his or her privacy has been compromised.

H(4). Government intrusion concerns are negatively related to the willingness to provide personal information to transact on the Internet.

The possibility of the government conducting unobtrusive or surreptitious surveillance increases the information asymmetry between individuals and the state. This asymmetry increases the perceived risk that access and possible abuse of the personal information by government institutions may occur. Individuals who develop concerns about government surveillance will be more likely to have greater privacy concerns. Perceived intrusion is related to both increased privacy concerns and behavior modifications (Kateb et al., 2001). These concerns stem from the probability that individuals will be objectified and oversimplified, taken out of context, or have part of their identity mistaken for the whole of their identity (Rosen, 2000). The positive relationship between perceptions about government intrusion and privacy concerns is also evident in the survey finding that one quarter of the public does not believe government will use its powers properly (Harris Interactive, 2003a,b). Moreover, scholars have recently argued that the balance between individual freedom and government intrusion is being tipped further away from individual freedom (Brin, 1998; Serr, 1994; Sundby, 1994). These considerations suggest the following.

H(5). Government intrusion concerns are positively related to Internet privacy concerns.

Government surveillance initiatives intended to ensure security may also result in concerns about the potential side effects of broadening the scope of government powers to monitor citizens. Etzioni (1999) refers to the latter as a slippery slope and categorizes the side effects into several classes: harassment and vigilantism, abusive utilization, unreliable data, and excessive intrusion into private transactions and behaviors. If an individual perceives these side effects to be present, then as government intrusion concerns increase, the perceived need for surveillance will decrease. The relationship might be characterized as one in which an individual observes that while surveillance might reduce the risk for the country as a whole, surveillance increases the risk for that individual in particular.

As a consequence, Internet users may object to government initiatives designed to increase surveillance. A reduction in public support for government surveillance may, in turn, undermine government efforts to increase protection for the public.

H(6). Government intrusion concerns are negatively related to perceived need for government surveillance.

4. Methodology and results

The model was empirically tested using data collected from a survey. We relied on the Dinev and Hart's (2004, 2006a) instrument for measuring Internet privacy concerns and willingness to provide personal information to transact on the Internet (PPIT) with slight modifications (the items used are shown in Appendix A). They reported two distinctly different dimensions of privacy concerns: privacy concerns related to information finding (PCIF) and privacy concerns related to information abuse (PCIA). Indeed, while using the Internet, individuals may be concerned that their private information may be found by third parties or unauthorized individuals without necessarily being maliciously used. In this case, the concern is based on the fact that the information is available and can be easily found. The other type of privacy concern, information abuse, addresses the specific anxieties related to information misuse and/or abuse.

In our search for empirical measures on surveillance-related constructs we explored the literature in social sciences, political economy, sociology, and organizational sciences, and contacted leading researchers in these fields. We were not able to find any previously developed and validated instruments that measure public beliefs

towards surveillance or any similar latent constructs. Consistent with the current best practices in scale development, we cast a wide net in identifying candidate items. We constructed an initial set of items reflecting the underlying theory while observing the trends in general survey research (e.g., Harris Interactive and Westin, 1991–2003) and following the analyses in the professional and popular literature. All of the items use a 5-point Likert scale. Initial report of the instrument development and validation is reported in Dinev et al. (2005) and cross-cultural differences were explored in Dinev et al. (2006).

Two pilot tests preceding the final survey were administered to a broad sample of individuals after September 11, 2001. The first pilot test was conducted among a sample of 100 respondents including MIS students from a large university and retail and service business employees in Southeastern United States. This was followed by a second pilot survey conducted among a sample of 70 undergraduate students at the same U.S. university. Following appropriate steps for measure development (Churchill, 1979), minor purification of the items was needed and the final instrument was validated at satisfactory levels (all items are shown in Appendix A). The final version of the survey was administered to a broad sample of individuals in Southeastern U.S. in two stages. The surveys were offered to students in classes, companies and institutions, and distributed door to door in neighborhoods off campus. Participation was voluntary and completely anonymous. The respondents returned a completed survey in designated collection boxes in work places or by prepaid mail. In the first stage, 369 surveys were collected and during the second stage, one year later, an additional 53 surveys were gathered. The response rate was 45% as measured by the ratio of the number of the completed surveys returned to the number of the surveys initially distributed. The respondents worked in a wide range of occupations with about equal percentages (between 10% and 15%) from technology, finance, retail, services, education, and local/state/non-profit sectors, and about 5% homemakers. The demographic distribution of the 422 respondents reveals a diverse sample, comprising a wide range of age, income, education, and race, with almost equal representation of gender (Table 2). The model was also estimated on the initial and year later sub-samples. The results were the same attesting to the longitudinal consistency of the observed relationships.

4.1. Structural equation modeling

The research model was tested using Structural Equation Modeling (SEM) with LISREL. We used the two-step approach (Anderson and Gerbing, 1988; Gefen et al., 2000) to first assess the quality of our measures with the measurement model, sometimes referred as confirmatory factor analysis (CFA), and then tested the

Table 2
Descriptive statistics of survey respondents ($N = 422$)

Gender	Male	48.6%
	Female	51.4%
Race	White	57.9%
	Black	15.3%
	Hispanic	15.0%
	Asian	7.1%
	Other (incl. missing)	4.7%
Age	<20 years	13.0%
	21–30 years	58.1%
	31–40 years	17.3 %
	>40 years	11.6%
Education	High School or a University student	66.1%
	4 year college degree	17.5%
	Graduate degree	16.4%
Income	<$60,000	64.3%
	$61,001–$100,000	19.4%
	>$100,000	13.7%
	Undisclosed	2.6%

hypotheses by estimating the structural (equation) model, also know as SEM. The CFA was performed on the entire set of items simultaneously with each observed variable restricted to load on its a priori factor.

Unlike first generation regression models and partial least squares (PLS), LISREL permits rigorous analysis of all the variance components of each observed variable (common, specific, and error) as an integral part of assessing the structural model. LISREL maps the specific and error variance of the observed variables into the research model. All the necessary steps to assess reliability and validitsy within the measurement model validation were conducted following Gefen et al. (2000), The maximum likelihood fitting function was employed for model estimation.

The CFA statistics are reported in Table 3 following widely accepted practices in the MIS literature (Gefen et al., 2000). The fit of the data to the measurement model was very good and the loading are all in the correct direction and statistically significant rendering it appropriate for analysis of the reliability and validity of the constructs and their measures. Reliability is necessary, but not sufficient to establish validity (Cook and Campbell, 1979) so we address reliability first and then validity.

4.1.1. Reliability

Reliability is established by estimating: (1) the internal consistency through Cronbach's alphas (recommended values > .70) and the squared multiple correlations (R^2) of the items and (2) unidimensionality through estimating the model's χ^2 (see Table 5), assessing unidimensionality is possible only with covariance-based SEM techniques and cannot be assessed using factor analysis or Cronbach's alpha (Gefen et al., 2000).

Cronbach's alphas' range from .84 to .94 providing support for the internal consistency of our model. Additionally, most of the R^2 are higher than .5 providing evidence of their reliability. Our model's χ^2 (Table 5) is insignificant and significantly smaller than alternative measurement models tested in our study, which supports the models' unidimensionality (Gefen et al., 2000).

4.1.2. Construct convergent validity

Convergent validity is established by: (1) adequate model fit indices such as GFI, NFI, AGFI, and χ^2; and (2) high factor loadings with high and significant *t*-values (Gefen et al., 2000). Construct (composite) reliability and average variance extracted (AVE) should also be estimated in that regard.

Table 3
Confirmatory factor analysis statistics

Latent variable	Item	Completely standardized latent construct loadings and error terms					*t*-value	R^2	Construct reliability	AVE
		PPIT $\alpha = .84$	PCIA $\alpha = .85$	PCIF $\alpha = .94$	PNGS $\alpha = .88$	GIC $\alpha = .92$				
PPIT	PPIT1	.89(.05)					22.30	.79	.91	.68
	PPIT2	.63(.05)					14.02	.40		
	PPIT3	.92(.04)					23.66	.85		
	PPIT4	.70(.06)					15.82	.49		
PCIA	PCIA1		.68(.05)				15.66	.47	.88	.72
	PCIa2		.98(.04)				26.39	.96		
	PCIA3		.85(.04)				20.91	.72		
PCIF	PCIF1			.85(.05)			21.53	.72	.97	.77
	PCIF2			.84(.05)			21.00	.70		
	PCIF3			.93(.04)			25.06	.87		
	PCIF4			.94(.04)			25.38	.88		
	PCIF5			.80(.05)			19.59	.64		
PNGS	PNGS1				.92(.05)		21.46	.90	.87	.64
	PNGS2				.72(.05)		15.75	.57		
	PNGS3				.84(.06)		16.86	.70		
	PNGS4				.69(.06)		13.68	.47		
GIC	GIC1					.83(.05)	20.44	.69	.91	.78
	GIC2					.90(.04)	23.09	.81		
	GIC3					.91(.05)	23.59	.83		

Our model's fit indices all exceed the recommended values for establishing convergent validity (Table 5). All the items exhibit large factor loadings (i.e., λs above .70) and high t-values demonstrating convergent validity (Bollen, 1989; Gefen et al., 2000). The recommended values for composite reliability are above .70 (Gefen et al., 2000) and the lowest composite reliability for our model is .87 (Table 3). Likewise, all estimates of AVEs (Table 4) are above .64, much higher than the recommended minimum value of .50 (Bagozzi and Yi, 1988). All of the above estimates provide further evidence of the scales' convergent validity. Therefore, all items are significantly related to their specified constructs.

4.1.3. Construct discriminant validity

Three techniques were used (Joreskog and Sorbom, 1989; Bollen, 1989; Mullen et al., 1996) to assess discriminant validity. First we examined whether the correlations between pairs of constructs (Table 4) were significantly different from unity providing evidence of discriminant validity (see also Gefen et al., 2000). The largest correlation of .62 was, as expected, between the two dimensions of PC, PCIA, and PCIF. The confidence interval for the .62, given a .03 standard error (.56 to .68), did not include 1.00, providing evidence that these are separate constructs. The other correlations (phis) were smaller with no confidence interval coming close to 1.00 indicating that each construct is significantly different from any other. Second, for each pair of constructs we ran χ^2 differences test between the fixed (correlation between the constructs of the examined pair fixed to 1.00) and the free (correlation between the examined pair of constructs estimated free) solutions. In each case, the two values of χ^2 for the fixed and the free solutions were statistically different providing further evidence of discriminant validity. Third, discriminant validity may be supported by demonstrating that the items share more common variance with their construct than with other constructs (Fornell and Larcker, 1981). For this test, we examine the AVE for each construct compared to the squared correlation between the constructs. Table 4 shows the average variance extracted (AVE) on the diagonal. The correlations between the latent constructs are on the off diagonal elements of Table 4. For instance, the AVEs for PPIT and PCIA are.68 and.72, respectively, with their squared correlation equal to .13. As Table 4 shows, all of the squared correlations are substantially less than the corresponding AVEs providing additional evidence of discriminant validity. All three approaches demonstrate more than adequate discriminant validity of the constructs in the model.

Collectively, the CFA model fit indices, factor loadings, squared multiple correlations, and composite reliability suggest that the indicators account for a large portion of the variance of the corresponding latent constructs and therefore provide support for the reliability and validity of the measures.

Further, we reduced the likelihood of common methods bias threat (Podsakoff et al., 2003; Straub et al., 2004) by ensuring anonymity to the respondents assuring them that there were no right or wrong answers, and requesting that each question be answered as honestly as possible. Also, following Podsakoff et al. (2003), we determined the common method variance using Harman's single-factor test by simultaneously loading all items in factor analysis using Varimax rotation. All indicators showed high factor loadings and low cross-loadings. Each principal component explained almost an equal amount of the 79% total variance, ranging from 12.5% to 16.6%, with one factor (PCIA) explaining 22% of variance. This result indicates that our data do not suffer from common method bias. After verifying the measurement model was acceptable, we move to the second step of estimating the structural model that we discuss next.

Table 4
Latent variable statistics

	Mean	Std. Dev.	PPIT	PCIA	PCIF	PNGS	GIC
PPIT	3.13	.96	.68				
PCIA	3.86	.94	−.36(.05)	.72			
PCIF	3.43	1.08	−.38(.04)	.62(.03)	.77		
PNGS	4.00	.51	.22(.05)	−.11(.05)	−.15(.05)	.64	
GIC	3.13	.45	−.11(.05)	.31(.05)	.29(.05)	−.30(.04)	.78

The correlations and error terms ( ) are shown in the off-diagonal terms. The diagonal terms indicate the AVE for each construct.

Table 5
Goodness of fit assessments for the measurement and structural model

Goodness of fit measures	χ^2(df)	χ^2 per df	NFI	CFI	IFI	RFI	GFI	AGFI	RMR	RMSEA
Acceptable model standard	Non-sign.	<2.00	>.90	>.90	>.90	>.90	≈.90	>.80	<.055	<.080
SEM model	495.32(139)	3.56	.92	.94	.94	.91	.90	.86	.053	.075

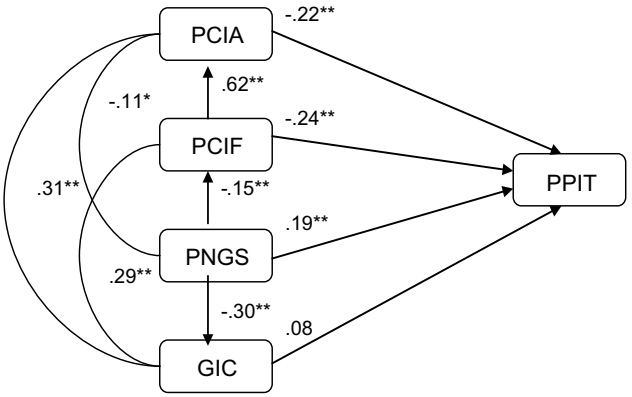

Fig. 2. Standardized parameter estimates of structural equation model. $^{*}p < .05$; $^{**}p < .01$.

4.1.4. Model fit

The results of fitting the structural model to the data show a converged, proper solution with a low χ^2 per degree of freedom. All the measures of fit (Table 5) were in the acceptable range and well above the minimum recommended values. These fit indices demonstrate a very good fit of the data to the model making it appropriate to evaluate the hypotheses with the resulting parameter estimates.

The completely standardized path coefficients in the structural model are used to evaluate the hypothesized relationships and are shown on Fig. 2. The parameter estimates for the hypothesized relationships within the model are statistically significant at the .01 level, except for the path from GIC to PPIT (H4) that is not statistically significant. These results provide support for five of the six hypotheses of the study.

5. Discussion

The primary goal of this paper was to develop and empirically test relationships between Internet privacy concerns, government surveillance beliefs, and how they influence the willingness to provide personal information to transact on the Internet. The analyses indicated that all the constructs' psychometric properties exceeded the established criteria for instrument reliability, and convergent and discriminant validity (Tables 3–5). The model's fit indices demonstrated its nomological validity suggesting that there are causal relationships among the factors in the model we tested. The results supported five of our six hypotheses with exception of H4 (Table 6).

5.1. Limitations of the study

Although the empirical results provide support for the study's model, some limitations should inform future research opportunities. The nature of the search for a balance between security and privacy within the context of the continuous flow of information technology advancements and their implementation in private and public institutions as well as the affect of procedures driven by unforeseeable political events requires longitudinal research. For that reason, our data collection was in two separate stages across one year period. Even though the results were consistent and the observed relationships held for each samples separately, more longitudinal studies are necessary to confirm the validity of the study. Perceptions of privacy are, arguably, very sensitive to government and corporate initiatives. And, perceptions are affected by the awareness of these

Table 6
Summary of the support for the hypotheses

Hypotheses	Hypothesized relationships	Support	SEM path coefficients	
H1	PC – PPIT (−)	Yes	PCIA −.22**	PCIF −.24**
H2	PNGS – PPIT (+)	Yes	.19**	.19**
H3	PNGS – PC (−)	Yes	PCIA −.11*	PCIF −.15**
H4	GIC – PPIT (−)	No	–	–
H5	GIC – PC (+)	Yes	PCIA .31**	PCIF .29**
H6	GIC – PNGS (−)	Yes	−.30**	−.30**

* $p < .05$.
** $p < .01$.

initiatives, among other factors. Thus, the results of our study are necessarily time bound. In this respect, our research must be viewed with the same caveat associated with so much research that focuses on the consequences of information technology and the rules whereby technology is used. The caveat is that the technology and the rules are ever evolving and thus their consequences may vary over time. The results of our analysis are only a snapshot of perceptions that may not be constant over time.

The theoretical model tested is broadly based on a privacy calculus framework in which the behavioral intention to disclose personal information is viewed as the result of a decision process or calculus, in which an individual weighs a set of salient competing antecedent factors. Our model does not incorporate a comprehensive set of factors; others have been assessed elsewhere (Dinev and Hart, 2006a,b). For example, social trust and personal interest have been found to be an important factor in the privacy calculus model, and also to explain and account for the cultural differences in attitudes toward government institutions (Dinev et al., 2005, 2006). Other potential factors include economic factors (saving time and or money), quality, and availability of relevant products and services. Additionally, the model and the survey instrument did not consider individual knowledge of government monitoring or the issues in general. The questions about government intrusion concerns asked about general concerns of potential surveillance and did not control for individual knowledge or awareness. Thus, a more comprehensive model with a larger set of factors should be considered in the future research.

The study suffers the common generalizability limitations due to demographic samples. The data were gathered primarily from Southeastern U.S.A. so there is the potential for national and or regional bias in the results. While we know of no reason to suspect regional difference, we should be aware of the potential of such since national differences based on culture have been explored (Dinev et al., 2005, 2006). We used a convenience sample which may limit the external validity and generalizability of the study results. We reached groups of Internet users with a wide range of demographic characteristics, so our large convenience sample approached the characteristics of a representative sample of Internet users as reported by Pew Research Center and other polling organizations. Future work needs to address this limitation by using more systematic approaches to sampling respondents.

5.2. Implications of the study

This study assessed the relationships among privacy concerns, the perceived need for government surveillance, government intrusion concerns and the willingness to provide personal information to transact on the Internet. While prior research has accounted for privacy concerns, to our knowledge this study is among the first to assess the influence of government surveillance factors, rather than only factors related to the gathering and processing of personal information by private institutions, in a statistically robust model. This is an important contribution.

The analysis provides a rigorous validation of the factors identified above. In addition, by placing the constructs in a nomological framework, the model provides support for the hypothesized the relationships and their relative importance for Internet use. Although time sensitive, the strong statistical results reveal a robust model that presents a relatively valid snapshot of the public beliefs while incorporating a broad theoretical justification.

Recent government initiatives to improve security following September 11th suggest that the information asymmetry between consumers and web retailers and third parties, including government agencies, has increased. Some of these initiatives enhance government authority to obtain personal information about consumers from private sector sources. This evolution in surveillance authority increases the panoptic power of the government. Internet technology provides an almost unprecedented opportunity for the unobtrusive surveillance of information related to personal interests. The perception that information gathering and analysis may be occurring could result in behavior modification regarding Internet use. At the same time, the need for security in an environment threatened by malicious intentions introduces a countervailing concern. The purpose of this research was to better understand how Internet users assess these concerns.

The data support the bifurcation of the Internet privacy concern construct, one related to concerns about information finding and the other related to concerns about information abuse. The relationships between each of these constructs and the other variables in the model were quite similar, in terms of direction and strength. In comparing the coefficients for privacy concerns about information abuse to privacy concerns about information finding, there is no more than a .05 spread between the standardized, statistically significant, coefficients. The consistently similar relationships for each of these privacy constructs suggests that individuals do not significantly differentiate between privacy concerns based on the potential threat of information abuse and simple information discovery. This is an interesting finding that deserves further scholarly exploration. One possible interpretation of the lack of differentiation may be that individuals believe that so long as information can be found on the Internet, the potential for abuse is not far removed. To the extent that this interpretation may be true, it surely reflects a negative assessment about the availability of personal information to be found on the Internet.

The results of our empirical study are consistent with the notion that government initiatives to improve security influence Internet use. The statistically significant relationship between perceived need for government surveillance and willingness to disclose personal information suggests that users perceive security initiatives as important and, arguably, tolerable. At the same time, government intrusion concerns do not directly influence willingness to provide personal information. However, government intrusion concerns are positively related to privacy concerns which, in turn, are negatively related to the willingness to provide personal information over the Internet. Thus, privacy concerns play an important role in understanding how users assess the relationship between government initiatives and Internet use. The negative relationship between perceived need for surveillance and government intrusion concerns further suggests that if government security-related initiatives were to be perceived as intrusive, the justification for such initiatives would decline. This would erode public support for government security initiatives and may, in turn, undermine government efforts to increase protection for the public.

These results are important and interesting for a number of reasons. The empirical support for the important role of privacy in e-commerce is consistent with other studies which show that privacy concerns inhibit online transactions (Culnan and Armstrong, 1999; Harris Interactive, 2003a,b; Dinev and Hart, 2003, 2004). The direction of these findings also reinforces the notion that disclosing how personal information is gathered and processed through online transactions is important to Internet users.

The findings regarding perceived need for government surveillance and government intrusion concerns suggest that the respondents of our survey were of two minds regarding government initiatives. The perceived need for government surveillance was positively related to willingness to disclose personal information and negatively related to Internet privacy concerns. On the other hand, government intrusion concerns were positively related to the Internet privacy concerns but did not affect willingness to disclose personal information. And, we found a negative relationship between perceived need for government surveillance and government intrusion concerns. A close examination of the items used to measure these two constructs shows that they are similar except for their orientation. The need for surveillance items were proactive statements addressing actions needed to be taken by the government. The intrusion concerns were statements about how actions would affect the respondents. Are the respondents saying: do what needs to be done to ensure security but we do not approve of what these actions will do to us or while security initiatives might be good for the country and e-commerce, they are not good me? There is an important nuance in these different interpretations.

The first interpretation would indicate that the respondents are uncertain about how to view the need for security initiatives. They are necessary but they have negative consequences and the resolution of this tension

is not clear. The second interpretation would indicate that the respondents acknowledge the need for security initiatives and that there will be negative consequences regarding privacy. The tension is not resolvable and therefore they will modify their behavior. It is not clear to us whether we can claim the accuracy of one of these interpretations over the other based on the data we have analyzed. However, the possibility of either begs for further study, especially because commercial surveys capture similar nuances (Harris Interactive, 2001, 2002, 2003a,b). They consistently indicate that, in spite of a relatively small decline in public support since 9/11, there is a broad consensus in favor of giving law enforcement increasing powers. At the same time, however, Harris surveys indicated that the public is anxious that certain initiatives pose threats to individual privacy – their primary message was Proceed – but with great care (Harris Interactive, 2001, 2002, 2003a,b).

The consistently mixed results of opinion polls about public attitudes toward surveillance since September 11, 2001, are in accordance with our findings. A recent poll about U.S. public support of the warrantless wiretapping program (Nagourney and Elder, 2006) provided particularly strong support for our results and interpretations of continuing mixed attitudes of the American public. According to the survey results, American citizens were willing to support a surveillance program if they believed it was intended to protect them. They however overwhelmingly opposed the same kind of surveillance if it was aimed at ordinary Americans. Thus, the majority of Americans approved of eavesdropping without prior court approval in order to reduce the threat of terrorism. When the same question was asked, but stripped of any mention of terrorism, the majority of the respondents said they disapproved.

An important implication of the study's results is that indeed a balance between the need for security and the fear about losing privacy exists in society. Maintaining this balance, through exercising vigilance, is crucial to avoid erosion of public support for government security initiatives. The potentially intensifying antagonism between privacy and security warrants a vigorous debate. The need for debate is further justified by two important trends: (1) surveillance technology is being adopted and used faster than public awareness of it and is outpacing the public debate, and (2) the public currently appears willing to sacrifice many aspects of privacy in order to combat terrorism (Gelbord and Roelofsen, 2002). At this stage, in the asymmetric information environment of the Internet, we speculated that many individuals are probably still using the Internet with cautiousness and awareness but without significant behavior modifications. The tip towards avoidance and resistance, however, can easily occur if further erosion of privacy is allowed. Surveillance policies and practices have to be masterfully crafted and justified to sustain use of information technologies like the Internet. The need for a new and redefined approach to privacy was identified even before the September 11th events – one that accords it equal standing with the common good, without privileging either value (Etzioni, 1999, p. 188).

The effort we are advocating in this study is focused on the particular artifact of Internet technology. Its inherent capability for transparent as well as unobtrusive data collection makes it an essential focus of research intended to better understand the balance between security and privacy needs. In the same vein, following the recent calls to focus on the IT artifact (i.e., Orlikowski and Iacono, 2001; Benbasat and Zmud, 2003), researchers interested in privacy concerns need to address the Internet tools used within particular and variant individual users' contexts and attempt to understand how privacy concerns are one among a number of antecedents that affect Internet use. For example, a fruitful direction for future research would be development of more nuanced measures of the different types of online transactions from a privacy perspective. As evident from the items used to measure willingness to provide personal information (Appendix A), our empirical study combines several possibly distinct behaviors into one theoretical construct. Although the assessment of convergent validity did not capture these nuances, the risks associated with disclosing credit card information in a sales transaction is arguably different than those associated with financial information, and needs to be further addressed.

Finally, asymmetric information theory has had a significant influence in shaping the direction of research in economics. Future researchers exploring the issues addressed here should consider drawing more closely on asymmetric information theory which holds that an increasing disparity in information between a principal, such as an Internet user, and an agent, such as an online retailer, should result in market failure. In the case of e-commerce, the asymmetry involves greater knowledge of the agent about how the personal information will be used. Moreover, the number of agents involved in e-commerce transactions is an issue that could be further assessed from this theoretical perspective. The market failure would be the refusal of the consumer to complete the online transaction or, if the transaction is completed, use of the personal information in ways that are unknown to the consumer, whether legitimate or otherwise. This theory could provide an important basis

for future investigations of the consequences of information technology for privacy, security and possibly other areas of concern to MIS researchers.

Appendix A. Items and scales

Latent variable	Item	Scale
Willingness to provide personal information to transact on the Internet (*PPIT*)	To what extent are you willing to use the Internet to do the following activities: *PPIT 1:* Purchase goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e., credit card information) *PPIT 2:* Retrieve information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates; or using sexual or gambling websites) Item-*PPIT 3:*Conduct sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software) *PPIT 4:* Retrieve highly personal and password protected financial information (e.g., using websites that allow me to access my bank account or my credit card account)	Not at all–very much
Internet privacy concerns for information abuse (*PCIA*)	How much do you agree with the following: *PCIA1:* I am concerned that the information I submit on the Internet could be misused *PCIA2:* I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee *PCIA3:* I am concerned about submitting information on the Internet, because of what others might do with it	Very low risk–very high risk
Internet privacy concerns for information finding (*PCIF*)	How much do you agree with the following: I am concerned that a person can find on the Internet: *PCIF1:* My date and place of birth, and the names of my parents *PCIF2:* Names and information about my immediate family members *PCIF3:* Address and telephone of my current and previous residences *PCIF4:* The location, the appraisal, and the price I paid for my assets/properties (house/apartment), as well as all the detailed information about my house *PCIF5:* My driving records	Not at all concerned–very concerned

(*Continued on next page*)

Appendix A (*continued*)

Latent variable	Item		Scale
Perceived need for government surveillance (*PNGS*)	How much do you agree with the following:		Strongly disagree–strongly agree
	PNGS1:	The government needs to have greater access to personal information	
	PNGS2:	The government needs to have greater access to individual bank accounts	
	PNGS3:	The government needs broader wiretapping authority	
	PNGS4:	The government needs to have more authority to use high tech surveillance tools for Internet eavesdropping	
Government intrusion concerns (*GIC*)	*GIC1:*	I am concerned about the power the government has to wiretap Internet activities	Strongly disagree–strongly agree
	GIC2:	I am concerned that my Internet accounts and database information (e.g., e-mails, shopping records, tracking my Internet surfing, etc.) will be more open to government/business scrutiny	
	GIC3:	I am concerned about the government's ability to monitor Internet activities	

References

Akerlof, G., 1970. The market for lemons: quality uncertainty and the market mechanism. Quarterly Journal of Economics 84 (3), 488–500.

Akerlof, G., 1977. The economics of caste and of the rat race and other woeful tales. The Quarterly Journal of Economics 90 (4), 599–617.

Anderson, J.C., Gerbing, D.W., 1988. Structural equation modeling in practice – a review and recommended 2-step approach. Psychological Bulletin 103 (3), 411–423.

BCG, Boston Consulting Group, 1998. Shop.org/BCG Survey of Online Customers. Available from: www.bcg.com.

Barbaro, M., Zeller Jr., T. 2006. A Face Is Exposed for AOL Searcher No. 4417749, New York Times, August 9.

Bagozzi, R.P., Yi, Y., 1988. On the evaluation of structural equation models. Journal of Academy of Marketing Science 16 (1), 74–94.

Benbasat, I., Zmud, R.W., 2003. The identity crisis within the is discipline: defining and communicating the discipline's core properties. MIS Quarterly 27 (2), 183–194.

Beniger, J.R., 1986. The Control Revolution – Technological and Economic Origins of the Information Society. Harvard University Press, Cambridge, MA.

Benn, S.I., 1982. Privacy, freedom, and respect for persons. In: Shoeman, Ferdinand David (Ed.), Philosophical Dimensions of Privacy: An Anthology. Cambridge University Press, Cambridge.

Bollen, K., 1989. Structural Equations with Latent Variables. Wiley, New York, NY.

Brin, D., 1998. The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?. Addison-Wesley Reading, Mass.

Campbell, J.E., Carlson, M., 2002. Panopticon.com: online surveillance and the commodification of privacy. Journal of Broadcasting & Electronic Media 46 (4), 586–606.

Cha, A., Krim, J., 2001. Privacy Trade-Offs Reassessed – Objections to Surveillance Technology Face New Test After Attack, Washington Post, September 13.

Chapman, G., 2000. The Privacy Cycle in American Politics, IT@IT – University of Texas at Austin. Available from: available at http://www.utexas.edu/computer/news/features/0110/chapman1.html. Last accessed August 31, 2007.

Churchill Jr., G.A., 1979. A paradigm for developing better measures of marketing constructs. Journal of Marketing Research 16, 64–73.

Clarke, R.A., 1988. Information technology and dataveillance. Communications of the ACM 31 (5), 498–512.

Clarke, R., 2001. 147 Congress records H8331, daily ed. November 16.

Clymer, A., 2003. Senate Votes to Curb Project To Search for Terrorists in Databases and Internet Mail, New York Times, January 24.

Cohen, J.E., 2000. Examined lives: informational privacy and the subject as object. Stanford Law Review 52 (1), 1373–1437.

Cook, T.D., Campbell, D.T., 1979. Quasi Experimentation. Rand McNally, Chicago.

Culnan, M.J., 1993. How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. MIS Quarterly 17 (3), 341–363.
Culnan, M.J., 2000. Protecting privacy online: Is self-regulation working? Journal of Public Policy and Marketing 19 (1), 20–29.
Culnan, M.J., Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization Science 10 (1), 104–115.
Culnan, M.J., Bies, R.J., 2003. Consumer privacy: balancing economic and justice considerations. Journal of Social Issues 59 (2), 323–342.
Davis, F.D., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly 13 (3), 319–340.
Dhillon, G., Backhouse, J., 2001. Current direction in IS security research: Towards socio-organizational perspectives. Information Systems Journal 11, 127–153.
Dinev, T., Hart, P. 2003. Privacy Concerns and Internet Use – A Model of Trade-off Factors, Academy of Management Meeting, Seatle. Best Paper Proceedings, OCIS Best Paper Award.
Dinev, T., Hart, P., 2004. Internet privacy concerns and their antecedents – measurement validity and a regression model. Behaviour & Information Technology 23 (6), 413–423.
Elsner, A., 2006. Privacy experts condemn subpoena of Google. Washington Post, January 20.
Dinev, T., Bellotto, M., Hart, P., Colautti, C., Russo, V., Serra, I., 2005. Internet Users' Privacy Concerns and Attitudes Towards Government Surveillance – An Exploratory Study of Cross-Cultural Differences Between Italy and the United States, 18th Bled E-commerce Conference, Bled, Slovenia, Outstanding Paper Award.
Dinev, T., Hart, P., 2006a. An extended privacy calculus model for E-commerce transactions. Information Systems Research 17 (1), 61–80.
Dinev, T., Hart, P., 2006b. Internet privacy concerns and social awareness as determinants of intention to transact. International Journal of Electronic Commerce 10 (2), 7–31.
Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., Colautti, C., 2006. Internet users' privacy concerns and beliefs about government surveillance – an exploratory study of differences between italy and the united states. Journal of Global Information Management 14 (4), 57–93.
Etzioni, A., 1999. The Limits of Privacy. Basic Books, New York.
Flaherty, D., 1989. Protecting Privacy in Surveillance Societies. University of North Carolina Press, Chapel Hill.
Fornell, C., Larcker, D.F., 1981. Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research 25, 186–192.
Foucault, M., 1983. The Subject and Power, second ed. University of Chicago Press, Chicago.
Gefen, D., Straub, D.W., Boudreau, M.C., 2000. Structural equation modeling and regression: guidelines for research practice. Communications of AIS, 4, Article 7.
Gelbord, B., Roelofsen, G., 2002. New surveillance techniques raise privacy concerns. Communications of the ACM 45 (11), 23–24.
Giddens, A., 1985. The Nation State and Violence. Polity Press, Cambridge.
Gilliom, J., 2001. Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy (The Chicago Series in Law and Society). University of Chicago Press (Trd).
Greenman, C., 1999. On the Net, Curiosity Has a Price: Registration, New York Times, December 23.
Grow, B., 2005. Hacker hunters: an elite force takes on the dark side of computing. Business Week 30 (May), 74–82.
Hafner, K., 2006. After Subpoenas, Internet Searches Give Some Pause, New York Times, January 25.
Hafner, K., Richtel, M., 2006. Google Resists U.S. Subpoena of Search Data, New York Times, January 20.
Harris Interactive., 2001. The Harris Poll: Overwhelming Public Support for Increasing Surveillance Powers and, In spite of Many Concerns About Potential Abuses, Confidence that these Powers would be Used Properly, October 3. Available from: http://www.harrisinteractive.com.
Harris Interactive, 2002. The Harris Poll: Homeland Security, April 3. Available from: http://www.harrisinteractive.com.
Harris Interactive, 2003a. The Harris Poll: Homeland Security, March 10. Available from: http://www.harrisinteractive.com.
Harris Interactive, 2003b. The Harris Poll: Most People are Privacy Pragmatists Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits, March 19. Available from: http://www.harrisinteractive.com.
Harvey, C., 1999. American Opinion (A Special Report): Optimism Outduels Pessimism, Wall Street. Journal, A10, September 16.
Hoge, W., 2001. U.S. Terror Attacks Galvanize Europeans to Tighten Laws, New York Times, December 6.
Hu, Q., Dinev, T., 2005. Is spyware an internet nuisance or public menace? Communications of the ACM 48 (8), 61–66.
Janofsky, M., 2002. Cities Wary of Anterior Tactics Pass Civil Liberties Resolutions, New York Times, December 23.
Joreskog, K., Sorbom, D., 1989. LISREL 7 User's Reference Guide. Scientific Software, Chicago, IL.
Kary, T., 2002. Government renews Cybercrime Push, CNET. Available from: http://news.com.com/2100-1001_3-836486.html.
Kateb, G., Rosen, J., Schauer, F., 2001. Invasions of privacy: violations of boundaries. Social Research 68 (1), 203–235.
Kelvin, P., 1973. A social-psychological examination of privacy. British Journal of Social Clinical Psychology 12 (3), 248–261.
Kling, R., 1996. Information technologies and the shifting balance between privacy and social control. In: Kling, Rob (Ed.), Computerization and Controversy: Value Conflicts and Social Control, second ed. Academic Press Inc., San Diego, pp. 614–633.
Kling, R., Allen, J.P., 1996. How the marriage of management and computing intensifies the struggle for personal privacy. In: Lyon, D., Zureik, E. (Eds.), Computers, Surveillance, and Privacy. University of Minnesota Press, Minneapolis, pp. 104–131.
Laudon, K.C., 1997. Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information, in Privacy and Self-regulation in the Information Age. U.S. Department of Commerce. Available from: http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1D.
Laufer, R.S., Wolfe, M., 1977. Privacy as a concept and a social issue: a multidimensional developmental theory. Journal of Social Issues 33 (3), 22–42.

Lichtblau, E., 2005. Social Security Opened its Files for 9/11 Inquiry. New York Times, June 22, p. 1.
Lichtblau, E., Share, S., 2006. Basis for spying in U.S. is doubted. New York Times, January 7, p. 1.
Liptak, A., 2002. In the Name of Security, Privacy for Me, Not Thee, New York Times, November 24.
Lyon, D., 1994. The Electronic Eye – The Rise of Surveillance Society. University of Minnesota Press, Minneapolis.
Lyon, D., 2001. Surveillance Society: Monitoring Everyday Life. Open University Press, Buckingham, Philadelphia.
Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research 15 (4), 336–355.
Margulis, S.T., 2003. Privacy as a social issue and behavioral concept. Journal of Social Issues 59 (2), 243–261.
Marx, G.T., 1998. An ethics for the new surveillance. The Information Society 14 (3), 171–185.
Marx, G.T., 2003. A tack in the shoe: neutralizing and resisting the new surveillance. Journal of Social Issues, 59.
Mason, R.O., 1986. Four ethical issues of the information age. MIS Quarterly 10 (1), 4–12.
Milberg, S.J., Burke, S.J., Smith, H.J., Kallman, E.A., 1995. Values, personal information privacy, and regulatory approaches. Communications of the ACM 38 (12), 65–74.
Milberg, S.J., Smith, H.J., Burke, S., 2000. Information privacy: corporate management and national regulation. Organization Science 11 (1), 35–57.
Milne, G., 2000. Privacy and ethical issues in database/interactive marketing and public policy: a research framework and overview of the special issue. Journal of Public Policy & Marketing 19 (1), 1–24.
Milne, G.R., Culnan, M.J., 2002. Using the content of online privacy notices to inform public policy: a longitudinal analysis of the 1998–2001 U.S. web sweeps. The Information Society 18 (5), 345–360.
Mullen, M.R., Doney, P., Becker, T., 1996. Time lagged effects of exporting and importing on economic development: replication and extension of mullen's 1993 model. Journal of Macromarketing 16 (2), 24–43.
Nagourney, A., Elder, J., 2006. New Poll Finds Mixed Support for Wiretaps, The New York Times, January 27.
Noam, E.M., 1997. Privacy and Self-Regulation: Markets for Electronic Privacy, in Privacy and Self-Regulation in the Information Age. U.S. Department of Commerce.
Nock, S., 1993. The Cost of Privacy: Surveillance and Reputation in America, New York.
Norris, C., Armstrong, G., 1999. The maximum Surveillance Society: The Rise of CCTV. Oxford, UK: Berg.
Orlikowski, W., Iacono, S., 2001. Desperately seeking the 'IT' in IT research – a call to theorizing the IT artifact. Information Systems Research 12 (2), 121–134.
Pavlou, P.A., Fygenson, M., 2006. Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. MIS Quarterly 30 (1), 115–143.
Phelps, J., Nowak, G.J., Ferrell, E., 2000. Privacy concerns and consumer willingness to provide personal information. Journal of Public Marketing 19 (1), 27–44.
Podsakoff, P.M., MacKenzie, S.B., Lee, J-Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of Applied Psychology 88 (5), 879–903.
Rather, J., 2005. In Huntington, Security vs. Privacy. New York Times, March 20, 2005, p. 11.
Rees, J., Bandyopadhyay, S., Spafford, E.H., 2003. PFIRES: a policy framework for information security. Communications of the ACM 46 (7), 101–106.
Rindfleish, T.C., 1997. Privacy, information technology, and health care. Communications of the ACM 40 (8), 92–100.
Risen, J., Lichtblau, E., 2005. Spying program snared U.S. calls. New York Times, December 12, p. 1.
Rosen, J., 2000. The Unwanted Gaze: The Destruction of Privacy in America. Random House, New York.
Rosen, J., 2001. Being Watched: A Cautionary Tale for a New Age of Surveillance, New York Times Magazine, October 7.
Safire, W., 2002. You Are a Suspect, New York Times, November 14.
Safire, W., 2004. Security with Liberty, New York Times, May 17.
Sanger, D., 2005. In address, Bush says he ordered domestic spying. New York Times, December 18, 1.
Serr, B.J., 1994. Great expectations of privacy: A new model for fourth amendment protection. Minnesota Law Review 73, 584–585.
Smith, H.J., 1993. Privacy policies and practices: inside the organizational maze. Communications of the ACM 36 (12), 105–122.
Smith, H.J., Milberg, S.J., Burke, S.J., 1996. Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly, 167–196.
Stadler, F., 2002. Privacy is not the antidote to surveillance. Surveillance and Society 1 (1), 120–124.
Starkey, K.P., McKinlay, A. (Eds.), 1998. Foucault, Management and Organization Theory: From Panopticon to Technologies of Self. Sage Publications, Beverly Hills, CA.
Stewart, K.A., Segars, A.H., 2002. An empirical examination of the concern for information privacy instrument. Information Systems Research 13 (1), 36–49.
Stone, E., Stone, D., 1990. Privacy in organizations: theoretical issues, research findings, and protection mechanisms. In: Rowland, K.M., Ferris, G.R. (Eds.), Research in Personnel and Human Resources Management, Vol. 8. JAI Press, Greenwich, CT, pp. 349–411.
Stone, E.F., Gueutal, H.G., Gardner, D.G., Clure, S., 1983. A field experiment comparing information-privacy value, beliefs, and attitudes across several types of organizations. Journal of Applied Psychology 68 (3), 459–468.
Straub, D., Boudreau, M.-C., Gefen, D., 2004. Validation guidelines for is positivist research. Communications of AIS 13, Article 24, 380–427.
Straub, D.W., Welke, R.J., 1998. Coping with systems risk: security planning models for management decision making. MIS Quarterly 22 (4), 441–469.
Sundby, S.E., 1994. Everyman's fourth amendment: privacy or mutual trust between government and citizen? Columbia Law Review (94), 1751–1752.

Swire, P.P., 1999. Financial privacy and the theory of high-tech government surveillance. Washington University Law Quarterly 77 (2), 461–513.
Swire, P.P., 2001. If Surveillance Expands, Safeguard Civil Liberties, Atlanta Journal Constitution, 21 October.
Swire, P.P., 2003. Efficient Confidentiality for Privacy, Security, and Confidential Business Information, in Brookings-Wharton Papers on Financial Services, 273-310.
Swire, P.P., Steinfeld, L.B., 2002. Security and privacy after september 11: the health care example. Minnesota Law Review 86 (15), 102–122.
Tolchinsky, P., McCuddy, M., Adams, J., Ganster, D., Woodman, R., Fromkin, H.L., 1981. Employee perceptions of invasion of privacy: a field simulation experiment. Journal of Applied Psychology 66 (3), 308–313.
Toner, R., 2001. Now, Government Is the Solution, Not the Problem, New York Times, September 30.
Toner, R., Lewis, N.A., 2001. A Familiar Battle Fought and Won, New York Times, October 26.
University of California, Los Angeles (UCLA). 2000, 2001, 2002, 2003, 2004. Internet report: Surveying the digital future. Available from: http://www.digitalcenter.org/.
Varian, H.R., 1997. Economic Aspects of Personal Privacy, in Privacy and Self-Regulation in the Information Age. U.S. Department of Commerce.
Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D., 2003. User acceptance of information technology: toward a unified view. MIS Quarterly 27 (3), 425–478.
Wald, M., 2004. Airline Gave Government Information on Passengers New York Times, January 18.
Walker, L., 2006. Forgot What You Searched For? Google Didn't, Washington Post, January 21, p. D01.
Westin, A.F., 1967. Privacy and Freedom. Atheneum, New York.
Westin, A.F., 2001. Opinion Surveys: What Consumers Have To Say About Information Privacy, Prepared Witness Testimony, The House Committee on Energy and Commerce, W.J. Billy Tauzin, Chairman, May 8.
Westin, A.F. with Harris Interactive, 2003. The Harris poll, March 19. Available from: http://www.harrisinteractive.com/harris_poll/index.asp?PID=365.