Internet Users' Beliefs about Government Surveillance – The Role of Social Awareness and Internet Literacy

Tamara Dinev, Florida Atlantic University, Boca Raton, USA
Email: tdinev@fau.edu

Abstract

This study focuses on exploring Internet literacy and social awareness as antecedents to Internet users' attitudes towards government surveillance in the Internet environment. Previously developed instruments for Internet literacy, social awareness, perceived need for government surveillance, and government intrusion concerns have been employed in the study. The relationships are measured and explored through Exploratory Factor Analysis (EFA) followed by linear regression models. Three of the four hypothesized relationships were found to be statistically significant - social awareness positively and Internet literacy negatively related to the perceived need for government surveillance, and Internet literacy positively related to the government intrusion concerns. The contribution of this research is in the attempt to explore surveillance attitudes in the post-9/11 American society. The study presents empirically tested relationships which are important for developing well-balanced policies of security protection and civil liberties.

1. Introduction

In the current American society, the phenomenon of data collection and processing is ubiquitous, prompting sociologists to argue that we live in a surveillance society [35, 41, 50]. Historically, the concept of surveillance is often associated with activities carried out by government agencies [15 35, 36]. However, the identification, collection, ordering, and categorization of personal information carried out by marketers in the private sector can also be regarded as surveillance. In particular, surveillance of online behavior is a fast-growing phenomenon that parallels the growth of Internet use. Both private corporations and government agencies take advantage of the increasing technical capability of information systems to profile consumers and citizens. They use these profiles to acquire knowledge about consumer preferences and citizen behaviors, for commercial purposes and for the prevention and detection of security breaches, fraud and other crimes, as well as terrorist activities. The prevalence of monitoring and profiling practices, regardless of their intentions, is indicative of a surveillance society [16].

In the years prior to September 11th, social scientists have noted that the public has attributed the source of threats caused by surveillance to the private sector rather than the public sector [4, 14, 29, 37, 40, 57, 59]. Data gathering and analysis activities of corporations, banks, lending institutions, credit card and marketing companies were perceived as the primary sources of intrusion and obliteration of privacy [5, 8, 9, 10, 27, 38, 39, 44, 45, 47, 54].

However, significant government actions were taken in response to September 11th. The efforts to improve security through surveillance are potentially changing U.S. citizens' attitudes towards surveillance. Government policy initiatives to monitor potential terrorist and crime activities are rapidly evolving in numerous ways, including with respect to the use of the Internet, wireless, and other digital media. In the U.S. alone, these initiatives include the Total Information Awareness Program amendment [7] the Patriot Act of 2001, the Homeland Security Act of 2002, and a series of executive orders, which give federal agencies greater authority to monitor individuals [26, 58]. The Cyber-Security Enhancement Act (CSEA) of 2002 govern the exchange of certain information collected in the private section to the agencies in the public sector. The CSEA allows government agencies to obtain e-mail, voice mail, phone records, Web-based transactions, and other services provided by the private sector.

Numerous polls after September 11 have found that security issues and the associated necessity of enhanced surveillance are becoming increasingly important [52, 53] with public opposition to greater government surveillance substantially muted [32]. At the same time, however, government policies may create antagonistic attitudes in its citizens who understand the need for security and protection but at the same time may be wary of loss of their civil liberties. For example, privacy advocates and civil libertarians have argued that these initiatives will increase the likelihood that personal information, such

1530-1605/08 $25.00 © 2008 IEEE

as credit histories, spending habits, unlisted telephone numbers, medical, employment and travel history, will be increasingly and more easily accessed without the individual's knowledge [31, 33]. There are growing concerns about the potential "side effects" - a "slippery slope" [14] of broadening the scope of government powers and prerogatives to monitor and profile citizens. The side effects may include unreliable data use, overly broad definitions of "potential threats" and investigatory nets, excessive intrusion into private transactions and behaviors, harassment and vigilantism [14]. One of the latest examples is the exponential growth of the federal government's "no-fly" list from 16 names on September 11, 2001 to more than 20,000 by October 10, 2004 [17] and the cases where it contained errors [18, 19]. The concern about government data collection and analysis has been expressed in perhaps the first scholarly paper published by an information systems researcher on the issue of privacy [38]. Thus, a balance between the need for preserving the civil liberties and the need for protection against crime and terror, reflecting current historical conditions, is vigorously sought.

These developments and the need to find the balance determine the need to understand the salient factors that are predictors of the citizens' attitudes. This will help in finding the delicate balance between the positive and negative attitudes towards surveillance that will ensure both social protection and public support of the government surveillance initiatives, while minimizing the threats to privacy and civil liberties.

In this study, two important factors of Internet literacy and social awareness as predictors of citizens' attitudes toward government surveillance are considered. The definitions and the measurement instruments of the Internet literacy and social awareness are adopted from [11] where these factors are included in an information privacy and Internet use model. The definition of government-related attitudes and the measurement instruments are adopted from [12] and [13]. In the theoretical section the constructs considered in the study are briefly introduced and defined. Then we argue that Internet users who have greater Internet literacy are more aware of the unprecedented means to unobtrusively observe activities and gather copious amount of information about individuals and their transactions. Thus, they will be more prone to develop concerns about government intrusion. These users will also feel less need to be protected by government security initiatives over the Internet since they believe they can handle security breach, identify criminal activity, etc. better than the average Internet user. From the other hand, the author argues that Internet users with higher social awareness will understand the higher needs for security and protection, thus exhibiting higher perceptions of need for government surveillance. At the same time individuals with higher social awareness will also be more concerned about potential effect on civil liberties and the negative consequences of intensified surveillance. Thus, they will also exhibit higher concerns for government intrusion. In the methodological section the hypotheses testing by linear regression are presented. The results are discussed in the Discussion section.

2. Theoretical considerations

The theoretical model of our study is shown on Figure 1. Short description and definitions of the construct is given below and the relationships among them hypothesized.

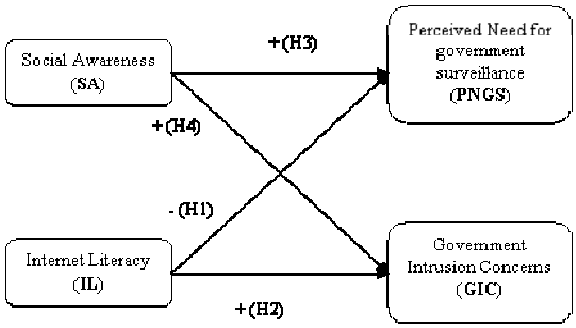

Figure 1. The study's Theoretical Model.

2.1. Beliefs about government surveillance

Internet technology facilitates information exchange with unprecedented speed and ease allowing a range of activities, both personal and business, to occur. Regrettably, they also facilitate various forms of criminal and harmful to the society activities, such as financial fraud, identity theft, offenses against minors, and so on. Taking into account the fact that terrorist activities are coordinated through active use of the Internet, the threats to the society and thus the need for more security cannot be understated.

In addition, the fact that the Internet is based on digital technology allows for the possibility of data acquisition not comparable to any other media. Transactions and communications conducted in cyberspace generate detailed electronic footprints that can easily be used to profile the individual, to expose his or her preferences, interests, and behaviors. The networked computer, connected to unknown parties, creates possibilities of unobtrusive monitoring of

online behavior by anonymous mediating parties. The latter include internet service providers, financial institutions, marketers, government agencies, etc. Many administer surveillance through the use of surreptitious techniques including tracking software installed in the Internet user's computer without his or her knowledge.

In this study, we consider two antagonistic beliefs about government surveillance that were initially developed by [12] and [13]. The first involves perceptions of the need for government surveillance which stems from the citizens' increased need for security, and the second involves concerns about government intrusion.

2.1.1. Perceived need for government surveillance (PNGS). The perceived need for government surveillance refers to the extent to which individuals assess the need to enhance security measures through surveillance to protect Internet users and to ensure safe and reliable Internet transactions [13]. Internet users are exposed to a high risk of information misuse and abuse. Unauthorized access to the personal computer and personal information can occur in several ways, including through hacking into computer systems, security defects and breaches, scams and spoof websites and email solicitations, uncontrolled secondary usage of personal data [47]. Malicious attempts to disrupt online service through viruses and other programs that threaten to destroy computer systems and networks or impede authorized access to databases can also be indications of attempts of criminal activities or terrorist actions. The dangers of such prompted Clarke [6] to refer to them as the danger of witnessing "digital Pearl Harbor". There has been less public tolerance for these risks since September 11th [28] and therefore, the average Internet user may perceive the presence of government surveillance as a beneficial factor protecting his or her online activities and e-service transactions.

2.1.2. Government intrusion concerns (GIC). Concerns about intrusions are related to the negative perceptions that individuals have about being monitored. Following [12], government intrusion concerns are defined as concerns about the government's ability to monitor and scrutinize an individual's use of the Internet. The mere knowledge that one is being observed changes his or her consciousness. Surveillance has social cost [48] and inhibiting effects on spontaneity, creativity, productivity, and other psychological effects. For example, Smith et al. [49] found that electronically monitored workers experience higher levels of depression, tension, anxiety, and lower levels of productivity than those who are not monitored, even when the monitored activities do not constitute private affairs.

Internet users may resist online information exchange for fear that their online activities may be recorded and stored and possibly become accessible to government agencies for subsequent scrutiny [49]. In this case their perceived need for security initiatives may be outweighed by the perceived negative consequences of possible intrusive surveillance. As a result, Internet users may develop objections to government initiatives designed to introduce greater security related to Internet use. This may, in turn, result in undermining government efforts to protect the public by reducing public support for government security initiatives.

2.2 Social awareness and internet literacy

The concept of Internet literacy was introduced by Dinev and Hart [11]. They argued that Internet users, while online, find themselves in a highly dynamic and interactive, networked environment where their computer and network experience depends on unknown third parties and intermediaries which unnoticeably, sometimes surreptitiously participate in the communication. Whether using email, chatrooms, discussion boards or simply browsing web sites, users face the need to manage situations which require substantial amount of technical skills from the users. Many of these situations have to do with commercial or government related surveillance. More and more Internet users are aware of their need to be able to handle deceptions [20], accidentally retrieved offensive content, spam email or spyware applications, etc. They realize that, in order to manage the ubiquitous surveillance, they need to have more thorough knowledge of how Internet operates, how to set the browser's privacy and security options, how to recognize phishing emails and spoof web sites, how to limit surreptitious gathering of personal information and behavior patterns, how to clean the computer system from parasite applications, viruses and worms [1, 30], how to keep up with the ever-going race between newer threats and updated protection. All this requires substantial amount of skills and knowledge in order to protect one's own computers, privacy, and information that would rather not be shared.

The Internet literacy can be expected to be closely related to computer literacy [34] but more complex, including the network-related factors mentioned above. Thus the definition of Internet literacy used in [11] is herein employed: Internet literacy is the self-assessed ability to use the Internet and various Internet-related applications to accomplish practical tasks by using a

computer connected to a network. A savvy Internet user who has the knowledge and skills to handle the above situations is also aware of the power of the government to gather data and track individual's web behavior. Such user, by knowing how to protect oneself and to control Internet attacks, would prefer to go on his own, perceiving less need to be protected by government security initiatives for the Internet. Thus, the more knowledgeable and Internet literate a user is, the less his or her perceived need for government surveillance will be. Concerned about his or her invasion of privacy, aware of the technical mechanism of surveillance and the government power of tracking, such a user will also exhibit a heightened state of government intrusion concerns. Therefore:

H1. Internet literacy negatively affects the perceived need for government surveillance.

H2. Internet literacy positively affects the government intrusion concerns.

There are many challenges about the Internet technology as a global phenomenon - technical (secure and reliable environment), regulatory (legal frameworks and standardizations), and social (trust, privacy, security, governance, censorship, restrictions) [3, 42]. Constant policy changes and improvements are driven by active engagement of citizens [55], by raising their awareness of how people affect the social environment. This engagement has been defined in the literature as social awareness. Social awareness [2, 21] is considered a key component of consciousness-raising related to the impetus of social change movements [2]. A person with high social awareness will tend to understand how a democracy works and exhibit interest in the U.S. political system and government or community policies [25, 51]. Previous research had linked social awareness to individuals' attitudes and cognitive development [43, 46, 56]. Dinev and Hart [11] found that social awareness is an important predictor to Internet privacy concerns. Following them, social awareness is here defined as the citizens' behavior with respect to following and being actively involved in communities' and government policies and initiatives, including those related to the technology and Internet.

Being socially active, Internet users with high social awareness would follow closely the problems of the Internet surveillance. Following news and highly publicized cases, they would also be more acquainted with the possible breaches of privacy, security and identity theft risks. They will tend to better understand the government's needs to provide protection mechanism and to limit the possibilities of crime and terrorist activities over the Internet. Being well informed, they will also tend to recognize to a greater extent the risks, legal and financial implications of intrusive government-regulated tracking of their behavior over the Internet, the possible consequences of the loss of privacy and negative consequences of scrutiny by an overzealous government agency. Thus, these users would have formed a stronger awareness about government surveillance, its importance and implications for the individual. The greater the citizenship engagement and social awareness of an individual, the greater importance that individual would place on both the need for security and the need for protecting the civil liberties as an important societal value. Therefore, one would expect that:

H3. Social awareness positively affects the perceived need for government surveillance.

H4. Social awareness positively affects the government intrusion concerns.

3. Methodology and hypotheses testing

The testing of the hypotheses was achieved through a survey administered to individuals in several stages during the years 2002-2004, in the Southeast of U.S. We approached students from a large southeastern university, teachers from 3 middles and 2 high schools, employees from 3 retail stores, 2 banking institutions and 25 high tech companies. The participation was completely voluntary. Participants were asked to fill the survey and drop it in a designated collection box. The average response rate across respondents from the different sectors, as measured by the ratio between the number of the distributed surveys and the number of the returned filled surveys, was 45%. The demographic profile of the 422 respondents revealed that the sample is diverse, with adequate representation of gender, race, employment, income, and age. Indeed, about 49% from the respondents were males and 51% females; 57% were white, 16% black, 15% hispanic and 7% asian (the remaining percentages are either "other" or "undisclosed"); 61% were less than 30 years old; 39% more than 30 years old. A large spectrum of employment sectors and occupations was captured (about equal percentage between 10% and 15% of the technology, finance, retail, services, education, state/government sectors). About 64% was with income less than $60,000, 20% between $61,000 and $100,000, and 16% more than $100,000. Thus the respondents were a heterogeneous group that may approximate a representative sample of a large population of Internet users.

This study used the instruments for measuring the constructs developed in [11]. For the reader's review, they are included in the Appendix. Factor analysis with Varimax rotation and Kaiser normalization was utilized to reassess the constructs' adequacy, with all items of the model run simultaneously in EFA (Table 1). All indicators loaded on the latent variables they were intended to measure, with insignificant cross-loadings of items. Furthermore, most of the factor loadings range between .82 and .92, as shown in the table, ensuring the face/content and factorial validity of the instrument. For further verification of discriminant validity, all inter-item correlations and crossloadings were examined. The values of the correlations between the items measuring different constructs were significantly lower than the correlations between the items measuring one and the same construct which suggests that both discriminant and convergent validity were reestablished for the constructs.

After validating the measures and the validity of the constructs as applied to the study's data, linear regression analyses were run for the government related constructs – PNGS and GIC – as dependent variables, and Internet technical literacy and social awareness as independent variables. The results from testing the four hypotheses are presented in Table 2.

Table 1. Exploratory Factor Analysis of All Constructs.

Item	IL	SA	PNGS	GIC
IL1	**.89**	.01	-.01	.00
IL2	**.92**	.04	.01	.02
IL3	**.89**	.10	.03	.07
IL4	**.89**	.07	.01	.00
SA1	-.01	**.85**	.00	.00
SA2	-.11	**.83**	.01	.03
SA3	.08	**.71**	-.06	.09
SA4	.11	**.84**	.15	.01
SA5	.21	**.68**	.08	.03
SA6	-.01	**.82**	.05	-.09
PNGS1	.03	.05	**.86**	-.11
PNGS2	-.10	.02	**.84**	-.09
PNGS3	.04	.04	**.87**	-.20
PNGS4	.07	.06	**.86**	-.08
GIC1	.04	.04	-.19	**.91**
GIC2	.00	.02	-.10	**.93**
GIC3	.04	.01	-.16	**.93**

Table 2. Results of Linear regression. * p<.05; ** p<.01. NS – not significant. The correlation between SA and IL is not statistically significant, therefore no moderating effects are observed.

	Social Awareness (SA)		Internet Literacy (IL)		R^2	df	F
	β	t	β	t			
PNGS	.17	3.16**	-.14	-2.54**	13.89	2	7.44**
GIC	NS	-	.29	3.98**	16.92	2	7.92**

4. Discussion

The purpose of this research study was to better understand how Internet users' attitudes toward government surveillance are related to the Internet technical skills of the Internet users, and their social engagement and awareness. The findings reported in the previous section suggest support for the three of the four hypotheses. As shown in Table 2, three of the four of the relationships indicated in the hypotheses are statistically significant at level .01. One of the relationships - the one stated in Hypothesis 4 – was found to be not statistically significant.

For each regression analysis the main effects were significant and accounted for 13.89% and 16.92% of the variance for the perceived need for government surveillance (PNGS) and the government intrusion concerns (GIC), respectively. The F values for both dependent variables were $7.44_{(2)}$ and $7.92_{(2)}$, respectively, both with $p<.01$.

Social awareness was statistically significant and positively related to the perceived need for government surveillance ($\beta = .17$, $t=3.16$, $p<.01$) and was not a statistically significant predictor of the government intrusion concerns. Thus, socially engaged individuals who are aware of the social and political processes in the society tend to exhibit higher perceptions of need for government surveillance for the Internet environment. However, these same individuals do not seem to exhibit higher concerns for government intrusion.

As hypothesized, the Internet literacy (IL) is negatively related to the perceived need for government surveillance and positively related to the government intrusion concerns. The relationship coefficient between IL and PNGS is $\beta= -.14$ ($t=-2.54$, $p<.01$), and the one between IL and GIC is $\beta= .29$ ($t=3.98$, $p<.01$). Indeed, savvy and technically literate Internet users are more likely to be able to handle and deny surveillance and privacy invasive technologies,

customize browsers' or Internet applications' options, eliminate processes of surreptitious software programs running on background, keep up with newest antivirus, anti-spam applications and be able to avoid government overzealous scrutiny. Therefore, by feeling that they have more control over the processes of their networked computers, such users' perceived need for government-initiated security through surveillance will be significantly lower. Simply said, they don't feel as much need for the government security protections through higher Internet surveillance. And in addition, users with higher Internet literacy are more worried about government intrusion and scrutiny practices. In that sense, higher technically literate users are more protective and uncompromising of their personal space being invaded by government online surveillance.

Although the results are provocative and most of the hypothesized relationships confirmed, there are limitations in the study itself. The study considered only two antecedents to public attitudes to government surveillance, while there could be more antecedents, such as privacy concerns, trust, etc. While the current study confirms the statistical significance of the relationships, they have not been tested within the nomological network of the other antecedents, so the relative importance of each antecedent can be estimated. Privacy and trust are well researched in the literature and should be included in further models. In addition, as with most empirical studies, the sample size and spectrum of respondents is a limitation. Even though an effort was made to include a range of different individuals representing different social groups of Internet users, the sample is limited to a certain geographical region of USA. A statistically random sample would have increased confidence in our results.

To the best of the author's knowledge, this is the first study which attempts to empirically capture the extent in which technically literate individuals and socially engaged Internet users perceive the need for government surveillance over the Internet use and transactions. In that sense, several interesting implications emerge. From the magnitude of the standardized regression coefficients, it is seen that the most strongly opinionated Internet users are the ones who are Internet savvy, understand the mechanisms of a networked environment, and thus can protect themselves. They exhibit highest concerns for government intrusion and feel less urgent need to submit to government surveillance for the sake of security and protection.

Second, Internet users who have high social awareness tend to support to greater extent government surveillance initiatives that would provide security and social protection. Having a better knowledge of government policies and practices, these users perceive that, in the age of high risks to the society from malicious attacks over the Internet, the government surveillance and need for profiling individuals is justified. An interesting observation is that these Internet users do not seem to develop concerns about government intrusion, despite vigorous debates in the media. A message similar to "Proceed but with care" [22, 23, 24] was not captured in this study among Internet users with high social awareness. Instead, one can argue that it is more likely to be the case of muted opposition to government surveillance as reported in [32]. It is hard to find the reason for this observation. It is probable that the users with higher social awareness are less individualists, are more society protection-oriented and thus tend to put the interests of the society before their own concerns. In other words, they may be more prone to the "if that's good for the society, then we have to do it" type of reasoning.

The study reveals two possible groups occupying the ends of the spectrum of attitudes toward government surveillance. The first group would be the one aversive to any type of government surveillance. This group would be populated by the technically savvy, relatively young Internet users with low social engagement and awareness. Having both low social awareness and high Internet literacy, these individuals will exhibit lowest perceptions of need for government surveillance – they will not be able to see the need or justifications for government surveillance. With highly running concerns for government intrusion, these individuals will object to surveillance-related government policies, would not support them and would be concerned about their privacy more than others.

The other end of the spectrum would be occupied by the group of Internet users who are highly engaged socially but have lowest Internet literacy possible. Such users would use the Internet in a limited way – email, browsing, purchasing, and would have no knowledge on how to protect themselves from online attacks. They would have high reliance on government protections – security policies, laws and regulations. Being aware of their helplessness, they would fully support the government surveillance practices which lead to more protections of the citizens and thus they would be ready to sacrifice their privacy. In the name of more protection and control, they would be ready to subject themselves to more scrutiny without raising intrusion concerns.

The importance of identifying these groups lies in the realization of the fact that in order to maintain public support for the government initiatives related to security and surveillance, both the Internet literacy and social awareness need to be addressed and increased,

so that the majority of the Internet users belong to the middle of the spectrum. These would be the individuals well informed and Internet literate – those who are able to protect themselves through guarding their own computer systems and personal information, but also who understand the need for enhanced government surveillance. Staying well informed and engaged, these individuals would be able to send the message "Proceed with care" to their government and would be in a better position to guard against excessive intrusion and "side effects" from overzealous government actions.

References

[1] Arthur, C. Hackers, shopfronts and worms: How fraud on the Internet costs customers £100,000 a day. *Independent*, November 11, (2003).

[2] Bickford, D. M. & Reynolds, N. Activism and service-learning: reframing volunteerism as acts of dissent. Pedagogy, *Critical Approaches to Teaching Literature, Language, Composition and Culture*, 8, 2, (2002) 229-252.

[3] Burn, J. & Loch, K. The societal impact of the World Wide Web – key challenges for the 21st Century. *Information Resources Management Journal*, 14, 4, (2001), 4-14.

[4] Campbell, J. E. and Carlson, M. "Panopticon.com: Online Surveillance and The Commodification Of Privacy." *Journal of Broadcasting & Electronic Media*, 46, 2002.

[5] Clarke, R.A. "Information Technology And Dataveillance," *Communications of the ACM* (31:5), 1988, pp. 498-512.

[6] Clarke, R. *147 Congress records H8331*, daily ed. Nov. 16, 2001.

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

[8] Culnan, M. J. "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly* (17:3), 1993, pp. 341-363.

[9] Culnan M.J. "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Direct Marketing* (9:2), 1995, pp. 10-19.

[10] Culnan, M. J., and Armstrong, P. K. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), 1999, pp.104-115.

[11] Dinev, T. and Hart, P. 2006. Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce*, 10, 2, 7-31.

[12] 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. Outstanding Paper Award, *18th Bled e-commerce conference*, Bled, Slovenia.

[13] 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.

[14] Etzioni, A. *The Limits of Privacy,* Basic Books, New York, 1999.

[15] Flaherty, D. *Protecting Privacy in Surveillance Societies*, Chapel Hill, Uni.of N. Carolina Press, 1989.

[16] Gilliom, J. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy (The Chicago Series in Law and Society),* University of Chicago Press (Trd), 2001.

[17] Goo, S. Faulty 'No-Fly' System Detailed, Washington Post October 9, 2004.

[18] Goo, S. Terror no-fly list singled out Kennedy. Washington Post, August 20, 2004.

[19] Goo, S. Committee Chairman Runs Into Watch-List Problem. September 30, 2004.

[20] Grazioli, S., Jarvenpaa, S. Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence, *International Journal of Electronic Commerce*, 7, 4 (Summer 2003), 93-118.

[21] Green, S. P., Kamimura, M. Ties that bind: enhanced social awareness development through interactions with diverse peers, *Annual Meeting of the Association for the Study of Higher Education*, Portland, Oregon, 2003.

[22] Harris Interactive, 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, 2001, available at http://www.harrisinteractive.com .

[23] Harris Interactive, The Harris Poll, "Homeland Security," April 3, 2002, available at http://www.harrisinteractive.com .

[24] Harris Interactive, The Harris Poll, "Homeland Security," March 10, 2003, available at http://www.harrisinteractive.com .

[25] Hepburn, M. A. What is our youth thinking? Social-political attitudes of the 1980s. *Social Education*, 49, (1985), 671-77.

[26] Janofsky, M. "Cities Wary of Antiterror Tactics Pass Civil Liberties Resolutions," *New York Times*, December 23, 2002.

[27] Jones, M. G. "Privacy: A Significant Marketing Issue for the 1990s," *Journal of Public Policy and Marketing* (10:1), 1991, pp. 133-148.

[28] Kary, T. 2002. "Government renews Cybercrime Push," CNET at http://news.com.com/2100-1001_3-836486.html

[29] Laudon, K.C. "Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information, in *Privacy and Self-Regulation in the Information Age*. US Department of Commerce, 1997.

[30] Levi, A. & Koc, C. Risks in email security, *Communications of the ACM,* 44, 8, (2001), 112.

[31] Lichtblau, E. "Aftereffects: Airline Safety; Government's 'No Fly' List Is Challenged In a Lawsuit," *New York Times*, April 23, 2003.

[32] Liptak, A. "In the Name of Security, Privacy for Me, Not Thee," *New York Times*, November 24, 2002.

[33] Loy, J. "Privacy Will Be Protected," *USA Today*, March 11, 2003.

[34] Luehrmann,A. Computer literacy-what should it be? The Mathematics Teacher, 74, (1981), 9.

[35] Lyon, D. *Surveillance Society: Monitoring Everyday Life*, Buckingham, Philadelphia: Open University Press, 2001.

[36] Marx, G. T. "The surveillance society: The threat of 1984-style techniques," *The Futurist*, (19:1), 1985, pp. 21-26.

[37] Marx, G. T. "A Tack In The Shoe: Neutralizing and Resisting The New Surveillance," *Journal of Social Issues* (59), 2003.

[38] Mason, R.O. "Four Ethical Issues of the Information Age," *MIS Quarterly* (10:1), 1986, pp. 4-12.

[39] McCrohan, K. F. "Information Technology, Privacy, and the Public Good," *Journal of Public Policy and Marketing* (8:1), 1989, pp. 265-278.

[40] Noam, E.M. "Privacy and Self-Regulation: Markets for Electronic Privacy, in *Privacy and Self-Regulation in the Information Age*. US Department of Commerce, 1997.

[41] Norris, C. and Armstrong, G. *The maximum Surveillance Society: The Rise of CCTV*, Oxford, UK: Berg., 1999.

[42] Papazafeiropoulou, A & Pouloudi, A. Social issues in electronic commerce: implications for policy makers. *Information Resources Management Journal*, 14, 4, (2001), 24-32.

[43] Perry, W. *Forms Of Intellectual And Ethical Development In The College Years: A Scheme*, Holt, Rinehart & Winston, New York, 1970.

[44] Petty, R. D. "Marketing Without Consent: Consumer Choice and Costs, Privacy, and PublicPolicy," *Journal of Public Policy and Marketing* (19:1), 2000, pp. 42-57.

[45] Phelps, J., Nowak, G.J, Ferrell, E. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Marketing* (19:1), 2000, pp. 27-44.

[46] Piaget, J. *The Equilibrium Of Cognitive Structures: The Central Problem Of Intellectual Development*. University of Chicago Press, Chicago, 1975.

[47] Rindfleish, T. C. "Privacy, Information Technology, and Health Care," *Communications of the ACM* (40:8), 1997, pp. 92-100.

[48] Rosen, J. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House, 2000.

[49] Safire, W. "You Are a Suspect," *New York Times*, November 14, 2002.

[49] Smith, M. J., Carayon, P., Sanders, K. J., Lim, Soo-Yee, LeGrande, D., "Employee Stress and Health Complaints in Jobs With and Without Electronic Performance Monitoring," *Applied Ergonomics*, 1992 (1), pp. 17-28.

[50] Stadler, F. "Privacy is not the Antidote to Surveillance" *Surveillance and Society*(1:1), 2002, pp.120-124.

[51] Steinem, G. *Outrageous Acts And Everyday Rebellions*. American Library, NewYork, 1983.

[51] Swift, J. S. Social consciousness and career awareness. *ASHE-ERIC Higher Education Reports*, 8. The George Washington University, School of Education, Washington D.C., 1990.

[52] Swire, P. P. and Steinfeld, L. B. "Security and Privacy after September 11: The Health Care Example," *Minnesota Law Review*, (86:1515), 2002, pp. 102-122.

[53] Taylor, H. "The Harris Poll," #17, March 19, 2003, available at http://www.harrisinteractive.com/harris_poll/index.asp?PID=365

[54] Thomas, R.E. and Mauer, V. G. "Database Marketing Practice: Protecting Consumer Privacy," *Journal of Public Policy and Marketing* (16:1), 1997, pp. 147-155.

[55] Tillman, B. Internet privacy legislation emerges: new legislation could bring U.S. privacy protection laws into step with those of the European Union. (Legislative & Regulatory Update). *Information Management Journal*, 36, 5, (2002), 14-18.

[56] Tsui, L. Effects of campus culture on students' critical thinking. *The Review of Higher Education*, 23, 4, (2000), 421-441.

[57] Varian, H.R. "Economic Aspects of Personal Privacy," in *Privacy and Self-Regulation in the Information Age*. US Department of Commerce, 1997.

[58] Wald, M. "Airline Gave Government Information on Passengers" *New York Times,* January 18, 2004.

[59] Westin, A. "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, 2001.

Appendix

Measurement Instruments for the study constructs (after Dinev and Hart 2006 and Dinev et al 2006)

Construct	Item Symbol	Item
Internet Literacy (IL)		Rate the extent to which you are able to do the following tasks:
	IL1	Identifying and deleting a program which you consider intrusive (spyware) and which was installed through the Internet without your knowledge and permission.
	IL2	Managing virus attacks by using antivirus software.
	IL3	Managing browser's privacy and security options
	IL4	Cleaning spyware and adware installations from your computer
Social Awareness (SA)		To what extent do you agree with the following:
	SA1	I am interested in reading political commentaries or watching them on TV.
	SA2	I closely follow developments in my community.
	SA3	I enjoy discussing important social issues with others
	SA4	I watch news and other television programs/channels that address current issues.
	SA5	I closely follow government regulations of high tech businesses.
	SA6	I read at least one newspaper everyday or watch news on TV.

Construct	Item Symbol	Item
Perceived Need for Government Surveillance (PNGS)	**PNGS 1**	The government needs to have greater access to personal information.
	PNGS 2	The government needs to have greater access to individual bank accounts.
	PNGS 3	The government needs broader wiretapping authority
	PNGS 4	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.
	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