

Internet Users' Privacy Concerns and Attitudes towards Government Surveillance – An Exploratory Study of Cross-Cultural Differences between Italy and the United States

Dinev, Tamara

Florida Atlantic University, Boca Raton, FL U.S.

tdinev@fau.edu

Bellotto, Massimo

University of Verona, Verona, Italy

massimo.bellotto@univr.it

Hart, Paul

Florida Atlantic University, FL 33431, U.S.

hart@fau.edu

Colautti, Christian

University IULM, Milano

christian.colautti@tesi.it

Russo, Vincenzo

University IULM, Milano

vincenzo.russo@iulm.it

Serra, Ilaria

Florida Atlantic University, Boca Raton, FL, U.S.

iserra@fau.edu

Abstract

This study examines cross-cultural differences in individual's privacy concerns and attitudes towards government surveillance as related to e-commerce use for Italy and the United States. We argue that for both cultures the user's decision to make a purchase is influenced by privacy concerns, perceived need for security provided by the government and the balancing concerns for government intrusion. The empirical model was tested using LISREL structural equation modeling. To better understand the differences across the two cultures for privacy perceptions and attitudes toward government, we incorporate dimensions from two of the most influential cultural theories – Hofstede's (2003) individualism/collectivism, and Fukuyama's (1995) theory of trust and social capital. The results support the hypotheses of the study in terms of direction and relative magnitude.

Keywords: e-commerce, privacy, government surveillance

1 Introduction

Sociologists have argued that the modern western societies are surveillance societies (Lyon 2001). The creation, collection and processing of data is a ubiquitous phenomenon. Both private corporations and government agencies take advantage of the increasing technical capability of information systems to gather, process, and store consumer and citizen data. They use this vast amount of data to build 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, and terrorist activities. These profiles provide numerous benefits but also introduce certain threats to information privacy and intrusion in personal space. The prevalence of monitoring and profiling practices – regardless of their intentions – is indicative of a surveillance society in which institutions gain power over individuals (Gilliom 2001).

At the same time, American legal precedent and public opinion also reflect a society in which privacy is highly valued as an expression and a safeguard of personal dignity (Cohen 2000; Laufer and Wolfe 1977; Rosen 2001; Swire 1999). The cross-country differences in privacy regulations are among the ten most important trends that will impact the Internet in the first decade of the 21st century (Erbschloe 2001). Privacy is among the highest of privileged individual rights (Etzioni 1999; Lyon 2001; Swire 2003; Westin 1975) and MIS researchers (Milberg et al. 2000, Bellman et al. 2004) have found that there are differences in information privacy concerns across cultures.

Numerous polls in recent years have found that security issues and the associated necessity of enhanced surveillance are becoming increasingly important (Swire and Steinfeld 2002; Taylor with Harris Interactive 2003) on both continents. Along with that an increase of privacy concerns has been triggered by the recent government initiatives following September 11th intended to improve security in response to the continuous threats of terrorism both in Italy and the United States. These initiatives have enhanced the surveillance authority of various government agencies to fight terrorist threats and are potentially changing the landscape of public sector-based privacy concerns vs. security needs with respect to the use of the Internet, wireless technologies, and other digital media (Swire 2001). These initiatives are an important catalyst for the debate about privacy among citizens of the U.S. (Toner and Lewis 2001), of European countries (Hoge 2001) and of other countries as well. The rapid evolution of the government initiatives to fight terrorism by enhancing surveillance have forced a social debate on consolidating security and privacy (“security *and* privacy”) rather than antagonizing (“security *vs.* privacy”) these two seemingly polar values (Safire 2004; Swire 2001; Swire and Steinfeld 2002).

Transactions conducted in cyberspace generate detailed electronic footprints that expose individuals’ preferences, interests, and behaviors. Thus, the Internet provides an unprecedented means to unobtrusively observe interactivity and to gather a copious amount of information about individuals and their transactions for both government and private sectors’ purposes. These developments pose an important challenge which we explore in our research model: what is the nature of the relationships and the balance between the need for enhanced security to ensure civil protection on the one hand and for addressing privacy concerns to ensure civil liberties on the other hand for both cultures?

This research is an exploratory study of privacy concerns and attitudes towards government surveillance as they are related to e-commerce use in United States and Italy. E-commerce use was chosen as a case of Internet use because of the higher need to surrender personal information and thus being potentially most privacy threatening activity on the Internet. The technological and regulatory conditions between the two countries are comparable and substantial cultural differences which may account for the difference in the decisions to submit personal information or to use the Internet as a whole and these are the focus of the study. Our objective is to study cross-national differences of privacy and attitudes towards government surveillance and examine how they affect e-commerce use and the willingness to provide personal information.

2 Cultural Differences Relevant to the Study

While in the global multicultural perspective both the U.S. and Italian societies are classified as western societies and as such belong to the group of low-context, individualistic cultures (Triandis 1989), a closer look and comparison between the two societies reveals important cultural differences that may account for the differences towards privacy concerns and attitudes toward government as a whole and government surveillance in particular. Compared to the United States, the Italian society is more high-context, collectivist (Gannon 2004), low-trust society (Fukuyama 1995, Gannon 2004, Harrison and Huntington 2000), which exhibits low propensity to trust to the social group's outsiders and low government and institutional trust. Fukuyama places the U.S. and Italy at the opposite poles of Fukuyama's spectrum of trust – the first being an example of a high-trust society, and the second, a representative of a low-trust society.

The major Hofstede's (1980, 2003) cultural indicator which affects the differences of the study's constructs between U.S. and Italy is the Individualism-Collectivism (IND) index (Italy -- 76, U.S. -- 91). Collectivism focuses on the basic level of behavior regulation of an individual's relationships with respect to others. In a collectivist society individuals regard the interest of the group as more important than the interest of any one individual. Thus, collectivists might display great loyalty to their group. They prefer cohesive and a tightly knit social fabric and rarely move in and out of groups. A society high on individualism implies a loosely knit society in which people consider themselves independent of others, pursue personal goals, move in and out of groups easily.

Attitudes toward government and government initiatives are related to the culture's propensity to trust. Higher levels of trust are evident in the social exchanges among group members in high collectivist cultures (Parks and Vu 1994, Hui et al. 1991). In these cultures one is unlikely to be trusting and cooperative with individuals outside of the group. Group membership influences whether a person or organization is trusted. On the other hand, the propensity to trust people in general, including strangers who are not from one's social group, has been shown to be larger among individuals in societies characterized by higher individualist orientations (Yamagashi and Yamagashi 1994, Inglehart et al. 1998).

Typically for a low-trust society, Italian families play a central role. The reliance on families as the sole source of trust and support is evident in the anthropological and historical features of Italy's evolution to modernity. For Italians, everyone is considered to be an outsider except members of the family. The distrust to the outsider is what Fukuyama calls "pervasive" (Fukuyama 1995). Banfield (1958) called the family-based isolation "amoral familism" and it remains a more powerful force throughout Italy – North, South, and center – as compared to North European and North American Societies (Fukuyama 1995). In the 10 year span of Euro-Barometer surveys (1976-1986), the Italian public from all the regions ranked lowest at every point in time in interpersonal trust among all other European countries (Inglehart 1990), although a remarkably pronounced and durable difference in trust exists among the various regions of Italy, the South (including Sicily and Sardinia) having lowest trust, twice lower in relative levels than the one of the Northern Italy.

Inglehart (1990) found that interpersonal trust and related cultural orientation were strongly linked with both economic development and stable democracy. It is important to note however, that while remaining still lower than any other European country, the levels of trust of all regions of Italy are experiencing substantial and rapid growth showing a rapid upward trend especially pronounced for the Northern Italy (Inglehart 1990, p. 35; Inglehart 1997). Starting from almost the incredible level of in 1959 (Almond and Verba, 1963), only 8 percent of the Italian public agreed that "most people can be trusted". The figure rose to 27 percent in 1981, and to 30 percent in 1986 and 38 in 1993 (Inglehart 1997). Following Inglehart, the economic growth and the increasing government stability may be largely explained by the increased levels of trust. Repeatedly occurring government and state corruption, familism, clientelism, patronage, and instability created a culture of poor government legitimacy, denunciation and institutional distrust in Italy (Dickie 2001, Bull 2001). Thus in general, we expect that the attitudes towards government and government surveillance in Italy will be shaped by the lower trust of Italians as compared to their U.S. counterparts. Indeed, confidence levels in most government and government-related institutions and functions, among which legal systems,

education, police, parliament, civil service, social security, and government in general is steadily lower for Italy in comparison to U.S. (Inglehart et al. 1998).

3 Constructs of the Study. Research Hypotheses

Internet Privacy Concerns. Privacy as a psychological construct and sociological issue has been researched by a wide range of scholars in different fields (Laufer and Wolfe 1977, Margulis 1977). All scholars (Margulis 2003) recognize its complexity and the existing dichotomy between the individual and others and explore its multidimensional, elastic, context-specific, and dynamic nature (Laufer and Wolfe 1977, Westin, 1975). Most of the extant MIS research involves employees' perceptions of privacy values and beliefs (e.g. Milberg et al. 2000, Smith et al. 1996). The explosive development of digital, Internet, and storage technologies has triggered MIS researchers' interest in privacy (Clarke 1998, Culnan 1993, Culnan and Armstrong 1999, Mason 1986). Privacy has been operationalized as privacy concerns (Culnan and Armstrong 1999, Milberg et al. 2000, Smith et al. 1996) which measure the anticipation of future possible loss of privacy. Previous research has confirmed that online purchase intent is most influenced by security (Su and Han 2003) and privacy concerns (Ranganathan and Ganapathy 2002, Dinev and Hart 2003, 2004). Privacy concerns are the single most cited reason for declining to use the Internet (Westin 2001). According to a series of UCLA Reports (2000-2004), privacy and the requirement to submit personal information are the primary factors that discourage users from shopping online. In this study we define Internet privacy concerns as concerns about possible loss of privacy as a result of a voluntary or surreptitious information disclosure to an online business.

The concept of privacy is related to the extent that individualism is sought after and reinforced in a culture (Etzioni 1999). The perception of space is associated with the notion of privacy (Laufer and Wolfe 1977). What is private and what public space, as well as how much physical distance between people is considered normal, are related to perceptions of privacy (Hall and Hall 1990). In the U.S., a highly individualistic society, legal precedent and public opinion highly value privacy as an expression and a safeguard of personal dignity (Laufer and Wolfe 1977) and individual right (Etzioni 1999, Westin 1975). The U.S. ranking of first among individualistic societies has been confirmed by other empirical studies (Rhee et al 1996, Triandis 1995).

In comparison, the relatively high collectivism and low-trust nature in Italy is expressed in very close, emotional family relationships (Fukuyama 1995, Gannon 2004). The family is considered the greatest resource and protection of all troubles. Family connections are extremely important in one's career success, company success, job hiring (Passerini 2004). Family loyalty is automatically expected and even geographical separations are generally not accepted well, even when they are due to job promotions, marriage, studying abroad, etc. (McGoldrick 1982). Therefore the concept of privacy is practically non-existent within the family. The family structure, along with the catholic religion (Hofstede 2003) obliterates personal space (Wilde-Menozzi 2003). A broad public discussion has been recently active on the threats to citizen privacy in the age of digital technology but this again is directed towards circles outside the immediate family and to large corporate businesses (Stella 2004). Linguistically the word "privacy" is borrowed from English because of its non-existence in the Italian language. The Italians' communication patterns in public, whether in public gatherings or waiting lines, allow for smaller personal physical space between individuals than for individuals in the U.S. The Italians' relatively higher necessity of voice communications and love of conversation limits the chances of anything staying secret, including personal and business confidentiality, thus creating the phenomenon of externalization (Gannon 2004). Thus, privacy may be easily compromised.

Paradoxically, although Italy has a more collectivist culture in which individuals outside the group are less trusted, the cooperative element of the collectivist culture to reinforce mutual goals could be associated with a greater willing to disclose personal information that in cultures that are more individualistic, such as the U.S. We conclude that although Italians are members of a low-trust society, they will tend to surrender personal information more easily than individuals in the U.S. Once they trust the entity, they are comfortable with a lower state of privacy. Even though, in general, individuals in the U.S. tend to trust more easily, they are less comfortable with releasing personal

information and would prefer to keep such information within “their own space”. In summary, U.S. individuals have a higher regard for privacy compared to individuals in Italy.

H(1) Internet privacy concerns are negatively related to e-commerce use for both cultures, the relationship being stronger for the individuals in the U.S.

Justification for government security. The need for government security is based on the risks related to the Internet environment in particular and the surveillance society in general. The risks come from two sources: unauthorized access to digitized information and harm 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). Harm to the infrastructure is related to 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. There has been less public tolerance for these risks since September 11th (Kary 2002) and their importance and possibility led Clarke (2001) to refer to the danger of someday witnessing a “digital Pearl Harbor”.

The perceived justification for government security then is defined as the belief that the government needs to increase security procedures to protect Internet users 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.

The post-9/11 trauma of the U.S. American public enhances its perceptions that the government needs to take the necessary steps, even at the expense of limiting certain civil liberties through broader and more intense surveillance, to secure the safety of the public spaces in general and the Internet as a digital medium. This, coupled with the general higher trust to government institutions and their role in providing security and safety, we can argue that:

H(2) Justification for government security is positively related to e-commerce use, the relationship being stronger for U.S. individuals.

Government Intrusion Concerns. Internet technology facilitates information exchange with unprecedented speed and facility allowing a range of activities to occur. These activities include personal exchanges and business transactions. Regrettably, they also facilitate various forms of criminal and harmful activities, such as financial fraud, identity theft, offenses against minors, and so on. Terrorist use of the Internet means that it is at the intersection of concern among those who would seek to increase security initiatives and those who would advocate civil protections for individuals. In addition, the fact that the Internet is based on digital technology allows for the possibility of data acquisition that is not comparable to any other media. While the government initiatives represent a need to ensure security, there are growing concerns about the potential “side effects” of broadening the scope of government powers and prerogatives to monitor and profile citizens. Etzioni (1999) refers to the latter as a “slippery slope” and lists the possible side effects into several categories: unreliable data use, overly broad definitions of “potential threats” and investigatory nets, excessive intrusion into private transactions and behaviors, harassment and vigilantism. A balance between the need for privacy and the need for protection against crime and terror, reflecting current historical conditions, is vigorously sought.

Higher justification for security means that the government would have itself greater access to personal information and greater authority to conduct surveillance. When the government surveillance outweighs the perceived benefit component of the higher security, users will perceive that same surveillance as intrusion. Concerns about intrusions are related to the negative perceptions individuals have about being monitored and the consequences of surveillance for them. In our model, government

intrusion concerns are defined as concerns about the government's ability to monitor and scrutinize an individual's use of the Internet.

It is important to differentiate between the privacy concerns and the 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 consciousness of oneself. 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 cost (Rosen 2000) and inhibiting effects on spontaneity, creativity, productivity, and other psychological effects. Internet users will inhibit the extent of the information they exchange for fear that their online activities may be recorded and stored and possibly become accessible to government agencies for subsequent scrutiny (Safire 2002). The justification for security initiatives is outweighed by the perceived negative consequences of possible intrusive surveillance. This may result in avoidance of the information disclosure required to complete e-commerce transactions.

Because of the lower trust in government in general, we posit that Italians will exhibit lower tolerance towards government surveillance and thus the government intrusion concerns will be more strongly related to the Internet use.

H(3) Government intrusion concerns are negatively related to e-commerce use, the relationship being stronger for Italians.

The consequences of acquiring additional information and the possibility of unobtrusive or surreptitious surveillance introduce a high risk component. The risk is that the security initiatives will increase access and possible abuse of the personal information obtained. Thus we expect that intrusion concerns should increase privacy concerns. Perceptions about government intrusion related to the side effects mentioned above give rise to privacy concerns. For example, one quarter of the public does not believe government will use its powers properly (Harris Interactive 2003). Scholars have argued that the delicate balance between individual freedom and government intrusion is being tipped further from individual freedom (Brin 1998; Serr 1994). Perceived intrusion is thus related to both increased privacy concerns and behavior modifications (Kateb et al. 2001).

U.S. culture, being highly individualistic and privacy oriented, would exhibit higher privacy concerns when government intrusion concerns are present. Thus:

H(4) Government intrusion concerns are positively related to Internet privacy concerns, the relationship being stronger for U.S. individuals.

The more an Internet user is concerned about being monitored, the greater the perceived threat to privacy and, in turn, the less the perceived need for initiatives which could reinforce outside monitoring. As government intrusion concerns increase, the justification for security initiatives decreases. The relationship might be characterized as one in which an individual observes that while security initiatives might reduce the risk for the country as a whole, surveillance increases the risk for an individual in particular. As a consequence, Internet users may object to government initiatives designed to introduce greater security related to Internet use. A reduction in public support for government security initiatives may, in turn, undermine government efforts to increase protection for the public.

Again in this case, the lower trust towards the government translates to lower tolerance towards government surveillance among Italians. Thus we can expect that as government intrusion concerns grow, the perceived justification for government security will be much less among Italians than among their U.S. counterparts.

H(5) Government intrusion concerns are negatively related to the justification for government security, the relationship being stronger for Italians.

4 Methodology and Results

The hypotheses were empirically tested using data collected from a survey. The Internet privacy instrument was taken from Dinev and Hart (2004), specifically the items measuring Privacy Concerns for Information Abuse and the Internet usage, including e-commerce, was adapted from Chau et al. (2002). The actual items were slightly modified from the original instruments to capture the context of this study. In our search for empirical measures on surveillance-related constructs we explored the literature in social sciences, political economy, sociology, and organizational sciences, and we contacted leading researchers in these fields. We were not able to find any previously developed and validated instruments that measure public attitudes towards surveillance or any similar latent variables. Consistent with the current best practices in scale development, we cast a wide net in identifying candidate items. Observing the trends in general survey data (ex. Harris Interactive and Westin 1991-2003), following the analyses in the professional and popular literature, while reflecting on the underlying theory, we constructed an initial set of items. All of the items used a 5-point Likert scale.

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 the Southeast of the United States. This was followed by a second pilot survey conducted among a sample of 70 undergraduate students at a large Southern US university. Following the same appropriate tests for data, minor purification of the items was needed and the final instrument was valid and consistent at satisfactory levels (items are shown in the Appendix).

The final questionnaire was translated from English to Italian by one of the study's authors, and back translated for accuracy. It was pretested with multiple respondents from Italy and U.S. who varied in age, gender and education. No major problems were identified, but an instrument refinement and few modifications in the translation followed. The survey was administered to broad samples of individuals from Northern Italy and the Southeast U.S. who were asked to voluntarily participate. The demographic distribution of the 889 participants from Northern Italy and 422 participants from the southeast of U.S. are presented in Table 1. As seen from the demographics distribution, the sample is diverse, comprising a wide range of age, education, with approximately equal representation of genders at least in the U.S.

Frequency	Gender (Female)	Age	Internet Experience(Years)
Italy	33.6%	<20 years – 23.2% 21-30 years – 63.9% 31-40 years – 9.4 % Other – 3.5%	< 2 years – 14.8% 2-5 years – 57.7% >5 years – 27.5%
United States	51.4%	<20 years – 13% 21-30 years – 58.1% 31-40 years – 17.3% Other – 11.6%	< 2 years – 9.1% 2-5 years – 43.3% >5 years – 47.6%

Table 1. Demographic information of respondents.

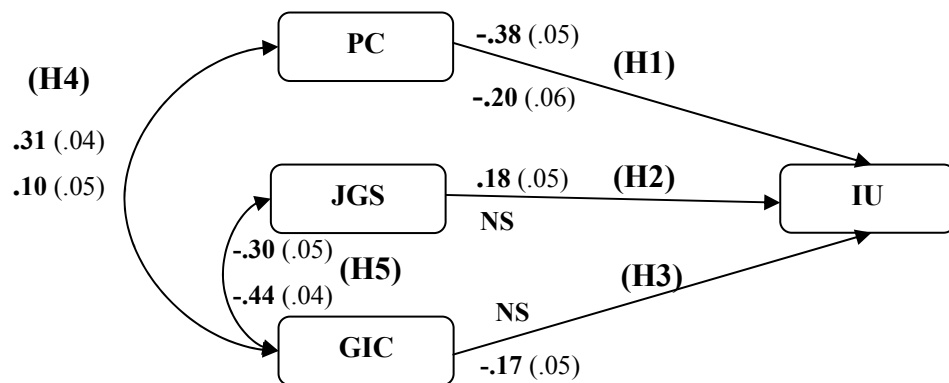
Measure validation for reliability was established through examining Cronbach's alpha coefficient for each construct, and discriminant and convergent validity was initially examined through exploratory principal component factor analysis with a Varimax rotation applied to all items simultaneously. All items loaded on their hypothesized constructors, with low, below .20 cross-loadings. A confirmatory factor analysis with LISREL was then conducted to further validate the measures of the principal constructs. The high factor loadings (above .60), composite reliability, and the average variance extracted (AVE) for each construct all confirmed the reliability, convergent and discriminant validity

of the instrument for both cultures (Table 2). Indeed, the square root of the AVE is much larger than all other cross-correlations for both samples, and both AVE and the composite reliability are higher than the recommended lowest limit of .60. Table 3 also lists the mean values and the standard deviations of the construct.

	ITALY				UNITED STATES			
	IU	PC	JGS	GIC	IU	PC	JGS	GIC
IU	.68 [.64]				.74 [.69]			
PC	-.20 (.04)	.94 [.87]			-.37 (.05)	.96 [.91]		
JGS	.08 (.04)	-.01 (.04)	.83 [.63]		.19 (.05)	<i>-.10 (.05)</i>	.87 [.77]	
GIC	.18 (.04)	<i>-.11 (.04)</i>	.42 (.04)	.86 [.80]	.08 (.05)	.31 (.05)	.28 (.04)	.84 [.78]
Cronbach's α	.78	.87	.84	.87	.77	.93	.88	.81
Mean values	1.51	3.47	2.12	3.66	4.2	4.43	4.00	3.13
Std. Dev.	.71	.70	.42	.68	.65	.52	.51	.45

Table 2. Latent Variable Statistics. Correlations with error terms () are the off-diagonal terms, and the composite reliabilities and the square root of AVE [] are the diagonal terms. Significant coefficients at $p < .01$ level are shown in bold, at level $p < .05$ in italics). **IU** = e-commerce use, **PC** = privacy concerns, **JGS** = justification for government security, **GIC** = government intrusion concerns.

In order to examine the hypotheses of the study, a structural equation modeling (SEM) with LISREL 8.0 was employed (Figure 1), allowing the estimation of the entire structural model for each country. The model resulted in a converged, proper solution with a low χ^2 and very good values of the fit indices for both countries (Table 3).



Top Coefficients: United States
Bottom Coefficients: Italy

Bold – $p < .01$
NS - not stat. significant

Figure 1. SEM completely standardized path coefficients, with error terms shown in ().

The path coefficients differences between the two SEM models (Figure 1) are statistically different, based on the t-test results, and are in the hypothesized direction. A more rigorous testing of the cultural effect is provided by the LISREL multigroup analysis through the χ^2 test. In this test, a model is analyzed in which the path coefficient between any two constructs of the model is constrained to have the value of the one in the corresponding model for the other culture. This constrained model's

(χ^2) is then compared to the original model's χ^2 where the correlation between the same two constructs was estimated freely.

Goodness of Fit Measures	χ^2 (d.f.)	χ^2 /d.f	NFI	CFI	IFI	NNFI	GFI	AGFI	RMR	RMSEA
Italy	189.85 (59)	3.22	.96	.97	.97	.96	.97	.95	.041	.050
U.S.	218.78 (59)	3.713	.93	.95	.95	.93	.92	.88	.055	.083

Table3. Model assessment indices for both cultures. LISREL notation applied.

Since the difference in degrees of freedom between the two models is 1, a difference in χ^2 greater than 3.84 suggests that the two constructs are statistically significant at level .05. This will prove cultural moderating effect. The results from the χ^2 tests on the relationships are shown on Table 4.

Construct Relationship	$(\chi^2)'$	$\Delta\chi^2$	Significance
IU-PC	205.47	15.62	.01
IU-JGS	213.61	23.76	.01
IU-GIC	279.00	89.15	.01
GIC-PC	247.62	57.77	.01
JGS-GIC	255.45	65.60	.01

Table 4. χ^2 test for culture moderating effect. $\Delta\chi^2 = (\chi^2)' - \chi^2$

5 Discussion

The findings of this study are in accordance with the theoretical model and the expectations related to the presented cultural arguments. The hypotheses of the study, the directions and relative magnitude of the path coefficients are supported by the empirical data. Thus we find that privacy concerns and Internet users' attitudes towards government surveillance are important predictors to intention to transact over the Internet for both cultures. In addition, the strong relationships between the privacy concern constructs and the government-related constructs indicate that these constructs are important components of any model that investigates surveillance and Internet use and aims to capture citizens' attitudes.

In particular, we find differences between Italy and the United States not only in the strength of the relationships as predicted by the hypotheses, but also that some of the relationships are not even statistically significant. Italians' Internet use for e-commerce purposes does not seem to be influenced by the justification for government security (H2). In other words, Italians seem to not feel a need for online government surveillance to make their online transactions. In contrast, Americans find that the government interference in making the Internet a safer environment facilitates their e-commerce use and they are more inclined to make online transactions, feeling more secure. As far as government intrusion concerns (H3), the Italian and U.S. landscape is opposite: the results suggest no statistical significance of GIC with e-commerce use for U.S. individuals, and a strong negative relationship for Italians. Thus, at this point of time, probably as post-9/11 traumatic reverberations, Americans seem to prefer the enhanced government surveillance for providing security rather than worry about government intrusion into the personal space of the individual. At the same time, however, while a

direct relationship is missing for Americans, the relationship between privacy concerns and e-commerce use and between GIC and privacy concerns is stronger than those for Italians. This is in accordance with hypotheses H1 and H4 but still reveals a mixed picture of the American attitudes. From one hand, the Americans' privacy concerns are higher and stronger related to e-commerce use and GIC, as expected from the higher individualism of the U.S. society. From the other hand, Americans do not seem to be bothered as much by concerns about intrusion from government – the latter raises their privacy concerns but does not affect directly their Internet use. The Italians, as expected from their attitude of low confidence in government in general, find government intrusion concerns inhibiting Internet use while raising to a lesser extent the privacy concerns. The explanation for that is the fact that privacy for Italians, as members of a relatively more collectivist society, is a weaker concept with a less role in the Italian's life. Finally, as predicted in H5, Italians' higher concerns about government intrusion lower the perceived need for government security significantly faster than with their U.S. counterparts.

The findings regarding perceived justification for government security and government intrusion concerns suggest that the U.S. respondents of our survey were of two minds regarding government initiatives, while the Italians were single-minded. A close examination of the items used to measure JGS and GIC shows that they are similar except for their orientation. The security justifications were proactive statements addressing actions needed to be taken by the government. The intrusion concerns were statements about how actions would affect the respondents. Thus the Italian respondents' message is coherent: "No need for government surveillance and interference here" while the U.S. respondents' message is more complex and mixed and needs further attention. Are the U.S. respondents saying: "do what needs to be done to ensure security but we don't 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 a slight 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 survey pools capture similar nuances (Harris Interactive 2001, 2002, 2003). 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, the surveys indicated that the public is anxious that certain initiatives pose threats to individual privacy. The surveys' primary message was "Proceed – but with great care" (Harris Interactive 2001, 2002, 2003).

An important implication of the study's results is that it reveals the delicate balance between the need for security and fear about losing privacy exists in society. Maintaining this balance is crucial for avoiding erosion of public support for government security initiatives.

References

- Almond, G. and Verba, S. (1963). *The Civic Culture: Political Attitudes and Democracy in Five Nations*. Princeton: Princeton University press.
- Banfield, E. C. (1958) *The Moral Basis of a Backward Society*. Glencoe, Ill.: Free Press
- Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20, 5, 313-324.
- Benn, S. I. "Privacy, Freedom, and Respect for Persons." *Philosophical Dimensions of Privacy: An Anthology*. Ed. Ferdinand David Shoeman. Cambridge: Cambridge University Press, 1982.

- Brin, D. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Addison-Wesley, Reading, Mass., 1998.
- Bull, A. C. (2001). Social and political cultures in Italy from 1869 to present day. In *Modern Italian Culture: The Cambridge Companion to Modern Italian Culture*, eds. Z. Baranski and R. West, pp.35-61. Cambridge University Press: Cambridge UK.
- Chau, P. Y.K, Cole, M., Massey, A.P., Montoya-Weiss, M. and O’Keefe, R. (2002). Cultural differences in the online behavior of consumers. *Communications of the ACM*, 45, 10, 138-143.
- Clarke, R. A. Information Technology and dataveillance. (1998) *Communications of the ACM*, 31, 498-512.
- Clarke, R. *147 Congress records H8331*, daily ed. Nov. 16, 2001.
- Cohen, J. E. “Examined Lives: Informational Privacy and the Subject as Object,” *Stanford Law Rev.* (52:1), 2000, pp. 1373-1437.
- 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. and Armstrong, P. K. (1999) Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, *Organizational Science*, 10, 1, 104-115.
- Dickie, J. (2001) The Notion of Italy, in *Modern Italian Culture: The Cambridge Companion to Modern Italian Culture*, eds. Z. Baranski and R. West, pp.17-33. Cambridge University Press: Cambridge UK.
- Dinev, T. and Hart, P. (2003). Privacy concerns and Internet use – a model of trade-off factors, Best Paper Proceedings of Annual Academy of Management Meeting, Seattle.
- Dinev, T. and Hart, P. (2004). Internet Privacy Concerns and Their Antecedents - Measurement Validity and a Regression Model, *Behaviour & Information Technology*, 23, 6, pp. 413-423.
- Erbschloe, M. (2001). Ten trends that will impact the Internet over the next five years, *Information Systems Management*, 18, 25-29.
- Etzioni, A. (1999). *The Limits of Privacy*, Basic Books, New York.
- Fukuyama, F. (1995). *Trust: The social virtues and the creation of prosperity*. NY: Free Press
- Gannon, M. J. (2004) *Understanding global cultures: metaphorical journeys through 23 countries*, 2nd Edition. Sage Publications: Thousand Oaks, CA.
- 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.
- Hall, E. and Hall, E. (1990) *Understanding cultural differences*. Yarmouth, ME: Intercultural Press.
- Harris Interactive, The Harris Poll, “Homeland Security,” March 10, 2003, available at <http://www.harrisinteractive.com> .
- Hofstede, G. (1980). *Culture's consequences: International differences in work-related values*, Beverly Hills, CA: Sage.
- Hofstede, G. (2003). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*, London, Sage.
- Hoge, W. “U.S. Terror Attacks Galvanize Europeans to Tighten Laws,” *New York Times*, December 6, 2001.
- Hui, C.H., Triandis, H.C., and Yee, C. (1991). Cultural differences in reward allocation: Is collectivism the explanation? *British Journal of Social Psychology*, 30,145-157.
- Inglehart, R. (1990) *Culture Shift in Industrial Society* Princeton University Press, Princeton NJ.

- Inglehart, R. (1997). *Modernization and Postmodernization: Cultural, Economic, and Political Change in 43 Societies*. Princeton University Press, Princeton NJ.
- Inglehart, R., Basanez, M. and Moreno, A. (1998). *Human Values and Beliefs: A cross cultural sourcebook*. Ann Arbor: University of Michigan Press
- Kary, T. "Government renews Cybercrime Push," CNET at http://news.com.com/2100-1001_3-836486.html
- Kateb, G., Rosen, J., Schauer, F. "Invasions of Privacy: Violations of Boundaries," *Social Research* (68:1), 2001, pp. 203-235.
- Laufer, R. S. and Wolfe, M. (1977). Privacy as a concept and a social issue: a multidimensional developmental theory. *Journal of Social Issues*, 33, 3, 22-42.
- Lipset, S. M. and Lenz, G. S. (2000). Corruption, Culture, and Markets. In *Culture Matters: How Values Shape Human Progress*, eds. Lawrence E. Harrison and Samuel P. Huntington, Best Books, New York, NY
- Lyon, D. *Surveillance Society: Monitoring Everyday Life*, Buckingham, Philadelphia: Open University Press, 2001.
- Margulis, S. T. (1977) Conceptions of privacy: current status and next steps. *J. of Social Issues*, 33, 5.
- Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *J. of Social Issues*, 59, 2, 243.
- Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, 10, 1, 4-12.
- McGoldrick, M. (1982) *Ethnicity and Family Therapy* New York: Guilford.
- Milberg, S. J., Smith, H. J. and Burke, S. J. Information privacy: corporate management and national regulation. *Organization Science*, 11, 1, (2000), 35-57.
- Parks, C.D., and Vu, A.D. (1994). Social dilemma behavior of individuals from highly individualist and collectivist cultures. *Journal of Conflict Resolution*, 38, 4, 708-718.
- Passerini, W. (2004) Italy is a land of string-pullers, *Corriere della Sera*, 17 June 2004.
- Ranganathan, C. and Ganapathy, S. (2002). Key dimensions of business-to-user web sites. *Information and Management*, 39, 457-465.
- Rhee, E., Uleman, J.S., and Lee, H.K. (1996). Variations in collectivism and individualism by ingroup and culture: Confirmatory factor analyses. *Journal of Personality and Social Psychology*, 71, 1037.
- Rindfleish, T. C. "Privacy, Information Technology, and Health Care," *Communications of the ACM* (40:8), 1997, pp. 92-100.
- Rosen, J. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House, 2000.
- Safire, W. "You Are a Suspect," *New York Times*, November 14, 2002.
- Safire, W. "Security with Liberty," *New York Times*, May 17, 2004.
- Serr, B. J. "Great Expectations of Privacy: A New Model for Fourth Amendment Protection," *Minnesota Law Review*, 73, 1994, pp. 584-585.
- Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20, 2, 167-196.
- Stella, G. A. "Tutti pedinati". Garante e cittadini senza privacy. *Corriere della Sera*, 1 August 2004.
- Suh, B., Han, I. (2003) The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce, *International Journal of Electronic Commerce*, 7, 3, 135-161.
- Swire, P. P. "If Surveillance Expands, Safeguard Civil Liberties," *Atlanta Journal Constitution*, 21 October, 2001.

- Swire, P. P. "Efficient Confidentiality for Privacy, Security, and Confidential Business Information," in *Brookings-Wharton Papers on Financial Services*, 2003, pp. 273-310.
- 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.
- Taylor, H. "The Harris Poll," #17, March 19, 2003, available at http://www.harrisinteractive.com/harris_poll/index.asp?PID=365
- Triandis, H. C. (1995). Individualism and collectivism. Boulder, CO: Westview Press.
- UCLA Internet report: surveying the digital future. (2000-2004), available at <http://ccp.ucla.edu/pages/internet-report.asp>
- Westin, A. (1975). Privacy and Freedom. Vintage, Ebury.
- 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.
- Wilde-Menozzi, W. Mother Tongue, An American Life in Italy. North Point Press, 2003.
- Yamagishi, T. and Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and Emotion*. 18, 129-66.

APPENDIX

Descriptive Statistics and Reliability Analysis of the Government Security and Government Intrusion Measures.

Item Symbol	Item	Mean	Std. Dev.	Corrected Item-Total Correlation	Perceived Justification for Government Security (GSJ)	Government Intrusion Concerns (GIC)
					Cronbach's $\alpha = .88$	Cronbach's $\alpha = .92$
GSJ1	The government needs to have greater access to personal information.	2.78	1.19	.75	.86	-.13
GSJ2	The government needs to have greater access to individual bank accounts.	2.31	1.12	.72	.84	-.11
GSJ3	The government needs broader wiretapping authority	2.74	1.28	.81	.87	-.21
GSJ4	The government needs to have more authority to use high tech surveillance tools for Internet eavesdropping	3.01	1.31	.72	.86	-.10
GIC1	I am concerned about the power the government has to wiretap Internet activities.	3.37	1.15	.82	-.17	.90
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	3.36	1.12	.86	-.11	.93
GIC3	I am concerned about the government's ability to monitor Internet activities	3.38	1.21	.87	-.17	.93