Information System Ethical Attitudes: A Cultural Comparison of the United States, Spain, and Portugal

Albert L. Harris  
*Appalachian State University, harrisal@appstate.edu*

Dave Yates  
*University of Maryland, dyates@umd.edu*

Jacqueline M. Harris  
*Appalachian State University, harrisjm@appstate.edu*

Rui Quaresma  
*University of Évora, quaresma@uevora.pt*

Follow this and additional works at: [http://aisel.aisnet.org/amcis2010](http://aisel.aisnet.org/amcis2010)

**Recommended Citation**

Harris, Albert L.; Yates, Dave; Harris, Jacqueline M.; and Quaresma, Rui, "Information System Ethical Attitudes: A Cultural Comparison of the United States, Spain, and Portugal" (2010). *AMCIS 2010 Proceedings*. 234.  
[http://aisel.aisnet.org/amcis2010/234](http://aisel.aisnet.org/amcis2010/234)

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2010 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Information System Ethical Attitudes: A Cultural Comparison of the United States, Spain, and Portugal

Albert L. Harris
Walker College of Business
Appalachian State University
Boone, NC 28608, USA
harrisal@appstate.edu

Dave Yates
College of Information Studies
University of Maryland
College Park, MD 20742 USA
dyates@umd.edu

Rui Quaresma
Department of Management
University of Évora
Évora, Portugal
quaresma@uevora.pt

Jacqueline M. Harris
Department of Mathematical Sciences
Appalachian State University
Boone, NC 28608, USA
harrism@appstate.edu

ABSTRACT
Ethical attitudes and behaviors of individuals influence information systems (IS) use. For organizations that operate across national borders, differences in ethical attitudes and behaviors will impact the actions of employees and customers. This research looks at the differences in attitudes and behaviors that exist among three different countries with distinct national cultures, and examines how these differences might impact information security. Building on existing ethical frameworks, we developed a set of ethical scenarios concerning data access, data manipulation, software use, programming abuse, and hardware use. We surveyed 537 students from three countries about their own ethical experiences and our ethics scenarios. The results indicated interesting differences among the countries that IS professions should be aware of when evaluating information and technology use for a multinational organization. We conclude with implications for current research and future research dimensions to further explore the impact of these differences.

Keywords
Ethics, ethical attitudes

INTRODUCTION
Researchers, practitioners, and policy makers are challenged with understanding the ethical implications of information and technology use between different geographical and cultural areas. Organizations that operate in many nations throughout the world face unique organizational challenges. Sometimes these challenges stem from conflicting technological standards, but more often due to a lack of awareness of different ethical expectations from one location to another (Lu et al., 1999; Volkema, 2004).

Sensibilities to laws, information security needs, responsibilities of employees to protect organizational assets, expectations that organizational employees act ethically with respect to information and technology use, and social and cultural norms for information and technology use can all differ depending on one’s cultural background. Many multinational organizations are tasked with instituting policies across national borders and must be aware of different ethical attitudes between representative nations. For example, Singh et al. (2007) report how married couples and members of collectivist communities such as Australian aboriginal groups routinely share confidential passwords and pins, despite bank warnings that such information must be kept private. Another example is the conflicting records management practices in US states with so-called “sunshine laws” such as Florida and Ohio (Sitton 2006) which mandate open access to records that contain personally identifying information, compared to states and nations which take the exact opposite approach with government records and tightly
control them. Even governments have difficulty creating and maintaining international policies despite existing structures to manage such efforts (Whitmore et al., 2009). Thus multinational organizations must be sensitive to local laws and must institute policies which will allow them to successfully interface with local populations. Often laws alone cannot help organizations identify differences, but a better understanding of the needs and expectations of users (internal, such as employees, and external, such as customers) might provide needed insight (Mitrakas, 2006; Sitton, 2006).

Recent evidence suggests that investigating ethical attitudes and behaviors might shed light on the formulation of organizational policies for a particular culture, country, or region (Elkin-Koren 2000; Huff & Martin, 1995; Lu et al., 1999). Research on ethical attitudes and behaviors that is based on experiences in one nation or another is helpful in identifying potential differences, yet cannot reveal the relative attitude and experience differences that might arise when specific events occur simultaneously in different nations. For example, policies to prevent illegal copying of software within an organization such as a university or a corporation may be completely effective in one nation, and completely ineffective in another, despite the best intentions of policy drafters and thorough understanding of the relevant information and technology issues involved in making such a policy.

In this paper, we describe a study of ethical attitudes and behaviors among students from three different nations using narrative scenarios that described events ranging from ethical policies and behaviors to computer crimes. We used the results to draw conclusions regarding the impact that differing ethical attitudes might have on information systems security policy.

BACKGROUND
Rest (1986) posited a simple ethical decision making process model consisting of four components. As a basis for a model for our study, we have modified this model to include the cultural impact on the process. Our adapted model is shown in Figure 1.

![Ethical Decision Making Model with Cultural Impacts](image)

Culture impacts every aspect of users’ ethical decision making with information systems. First, culture impacts what we recognize as a moral issue. In some cultures, software piracy or illegal downloading of copyright songs is not considered an ethical or moral issue. Second, culture establishes how we make a moral judgment. In some cultures, copyright is recognized by law, but not enforced in society. Although someone might recognize software piracy or illegal downloading of copyright songs as a moral issue, they might make the moral judgment that it is acceptable in their culture to proceed to actually download the song. Third, culture becomes a basis for the establishment of moral intent. Internet gambling is illegal in some countries (including the United States), but the culture provides a basis for the intent to break the law. The Internet site is outside my country and I am not hurting anyone; therefore I have no moral obligation to obey the law. Finally, culture becomes an incentive to engage (or not to engage) in moral behavior. For example, the culture for people who live in a poor country is to use all resources to their fullest. When a resource is available, they take it (often illegally) and use it without moral or ethical considerations. If copyright protection is not part of the country’s culture or laws, pirating software is not recognized as an ethical issue. People immediately make a moral judgment that software piracy is not bad (or illegal). The basis is established for illegal downloading of copyrighted songs when one goes to a site that allows illegal downloading. There is an incentive to engage in immoral or illegal behavior, such as the use of software that one has not purchased (Chellappa & Shivendu, 2005).

Colleges and universities throughout the world have also led the way in establishing information policies regarding ethics for their IS professionals, faculty, and students (Ben-Jacob, 2005; Fleischmann et al., 2009; Harris, 2000). Sometimes called a Computer Use Policy or Code of Ethical Behavior, these policies generally cover such areas as intellectual property rights, copyright laws, computer and data access, data use, data manipulation, and hardware use. Most colleges and universities
require employees and students to acknowledge and agree to comply with the policies before users are allowed to access the computing resources.

Ethics has become a part of many IS and business classes. It is important for students to understand the importance of ethics and the need for ethical behavior in all walks of life. Students who disregard ethical behavior will probably become employees that disregard ethical behavior. Thus our concern with ethics education is not only for students as end users, but also as future employees and policy makers in MNCs (Elkin-Koren, 2000). Finally, students have access to information technologies, the capacity to make mental judgments, and are generally active participants in the information society of their particular culture or nation.

**CULTURAL IMPACTS ON IS ETHICS**
In this section we present a discussion of the cultural impacts on IS ethics by looking at national culture and cultural differences.

**National Culture**
Cultural differences are an important issue when looking at IS ethics (Conger & Loch, 1995; Vitell et al., 2003). Culture manifests itself in heroes, rituals, symbols, and values. Legacy stories about heroes have been written and told many times over generations while rituals and symbols can be observed. Values, however, have their inherent virtues and they are hard to observe or describe.

Then exactly what is national culture? Hofstede (1980) defined it as a set of mental programs that control an individual’s responses in a given context. Parsons and Shils (1951) defined it as a shared characteristic of high-level social systems. Erez and Earley, (1993) defined it as the shared values of a particular group of people.

Classifying national cultures and identifying those dimensions that differentiate cultural behavior has been somewhat difficult and controversial. Hofstede (1980) provided one of the major studies on the subject. He found that national culture could be defined by four dimensions: power distance, uncertainty avoidance, individualism-collectivism, and masculinity-femininity. He later added long-term orientation as a fifth cultural dimension. Other studies, such as Project Globe, have confirmed Hofstede view that these dimensions and others can be used to differentiate behavior between cultures (Javidan and House, 2001). Each cultural dimension was quantified with a specific indicator to illustrate countries’ differences; however, long-term orientation scales are not available for all of the countries studied, so we have omitted that dimension in our analysis. Table 1 shows the index values for each of Hofstede’s initial four dimensions for the countries we studied: the United States, Spain, and Portugal.

<table>
<thead>
<tr>
<th></th>
<th>USA</th>
<th>Spain</th>
<th>Portugal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Distance</td>
<td>40</td>
<td>57</td>
<td>63</td>
</tr>
<tr>
<td>Individualism</td>
<td>91</td>
<td>51</td>
<td>27</td>
</tr>
<tr>
<td>Masculinity</td>
<td>62</td>
<td>42</td>
<td>31</td>
</tr>
<tr>
<td>Uncertainty Avoidance</td>
<td>46</td>
<td>86</td>
<td>104</td>
</tr>
</tbody>
</table>

Table 1: Hofstede’s Indexes for the Countries in the Study (Source: www.ClearlyCultural.com)

In addition to cultural differences, user expectations and user experiences have also been identified as factors that might impact actions at the individual level (Ben-Jacob, 2005; Huff & Martin, 1995). These individual factors also play a role in interpreting a company’s policies. User expectations and user experiences differ by country. Therefore, when looking at IS ethics in an organization, user expectations and experiences can cause interpretation differences based on one’s country of origin.

**Examining Cultural Differences**
In this study, we attempted to look at how differences in culture, user expectations and user experiences might manifest themselves. Would people from different countries respond differently to potentially unethical or criminal situations based on their cultural differences? How different are their actual past experiences and expectations with ethical/illegal situations? What factors might account for differences in how they might respond to ethical situations? Although we do not attempt to answer all of these questions, they provide a basis for our study.
Fleischmann (2007) noted that ethics and values can be embedded in technologies and digital services. Is it enough to design technology with ethics in mind, or do cultural differences necessitate further organizational decisions beyond technology design? Our study was designed to examine these differences through students’ responses to ethical scenarios. Through this study, we hoped to identify differences in IS ethical attitudes among students from different countries and cultures.

RESEARCH METHODOLOGY
We conducted a survey of ethical attitudes and behaviors among students at one university from three different nations. Each participant read a number of narrative scenarios and reacted to them as if they were observing the activity (e.g. viruses, file sharing, unauthorized systems access, etc.). In each scenario the participant evaluated whether the individuals involved acted ethically, acceptably but not strictly ethically, questionably, unethically, or illegally (broke the law). We also asked each respondent about their personal history with eight illicit activities concerning information and technology use. This allowed us to build an ethical profile for each participant and gauge their scenario responses against their personal ethical profile, their country of origin, and several other demographic factors.

Observing ethical dilemmas in real life, particularly on a large scale, is not feasible since most people encounter these situations surreptitiously and often when they are alone or in private. Even if observation were possible, it is likely that social desirability bias would skew the results. Therefore we utilized an anonymous survey methodology. This approach avoided generalization bias (Reis & Gable, 2000) sometimes encountered with hypothetical survey questions about ethical attitudes and practices. The survey contained specific scenarios that ranged from completely legal to illegal (although no indication of legality was given to the respondent). This approach is widely used in ethics research (Fleischmann & Wallace, 2005; Harris, 2000; Paradice, 1990) and in higher education, corporate and government ethics training (Ben-Jacob, 2005; Robbins et al., 2008).

A total of 537 students completed the survey between August 2005 and May 2007. Surveys were administered in a tight time frame at each institution since specific classes at each institution participated (most geared toward international business) rather than the whole institution. The survey was administered to all participants in English, the language used for instruction in each of the classes. Respondents were able to indicate any problems understanding the language or context of the survey in a free-form comment section and no respondent stated any difficulty comprehending or completing the survey.

Ethical Scenarios
We employed a set of 22 scenarios to reflect modern technology use. The survey was originally designed to map to Mason’s (1986) ethical issues of information privacy, information accuracy, information ownership, and information accessibility into computer use scenarios. Five types of scenarios were employed: data access, data manipulation, software use, programming abuse, and hardware use. These scenarios included peer to peer networking and file sharing, third party verification, and widespread SPAM. For example, a scenario given for the data access category is:

A salesperson believes that she is not being paid the same as other salespeople. She figures out how to access payroll records on the main computer. She reviews the pay of the other salespeople and the sales manager and concludes that she is getting paid appropriately. No other use of the information was made.

Some scenarios, like the one above, concerned gray areas of law or policy where it was not clear that the action was illegal, or even unethical. Other scenarios were designed to represent events that were illegal in some of the countries, either by specifically stating in the scenario that an illegal action was taken or by presenting a de jure illegal action. For example:

Gambling is illegal in the state or country where you are located. One of your co-employees, Jackson, uses his computer at work to access an off-shore website for gambling activity.

For each scenario, respondents rated the action of one or more involved scenario participants (such as the employee and the manager) or respondents rated multiple participant actions (such as downloading music and making and selling DVDs with that music). We chose the impersonal approach in which scenarios represent the actions of others (Paradice 1990; Wood 1993) rather than the personal approach (i.e. “you steal another user’s password…”) to allow for multiple participant roles in certain scenarios and to avoid self-relevant bias from participants imagining themselves in these situations (Reis & Gable, 2000). Respondents evaluated the participant actions on a five point scale: “Ethical,” “Acceptable,” “Questionable,” “Unethical,” or “Computer Crime.”
Ethical Profile
The survey included an ethical profile to quantify respondents’ actual experiences in potentially unethical or illegal situations. We asked a series of 8 questions about past and present activities reflecting the general categories of actions, such as downloading music without paying for it, changing data, knowingly releasing viruses, and illegal use of software. Since the set of questions listed activities across a range of situations that may or may not share one underlying theoretical justification (Fornell and Larcker, 1981), we considered it formative data. Therefore, we summed, rather than averaged, the scale to create an individual ethical profile. We summed these responses into an associative ethical profile, since it reflects respondents’ knowledge of unethical or illegal activities from their close associates. Each profile has a potential response range of 0 (no unethical/illegal activity reported) to 8 (respondent has done, or associates with those who have done, all of the activities listed).

Finally, we asked several demographic questions for comparative purposes. These included respondents’ age and gender, factors previously shown to impact responses to ethical situations (Harris, 2000), their year in school (1=freshman or 1st year, 5= graduate/post-graduate) and their knowledge of computers (1=very little or no knowledge, 5=extremely knowledgeable).

RESULTS
We first ran a country-wise comparison of the background characteristics to determine if these factors might be significant in our subsequent analysis of the scenario and ethical profile responses using SPSS 15.0 to compare age, gender, year in school and computer knowledge using country as a grouping variable. For age, our respondents from Portugal were significantly older than respondents from the USA, and Spain (p values < 0.01 to < 0.001). For year in school, respondents from Spain were significantly less advanced than those from the USA and Portugal (p values < 0.01 to < 0.001).

We next analyzed responses to our ethical profile questions. Table 2 lists the average values for Individual Ethical Profile and Associative Ethical Profile for the full sample and by country. Interestingly, only one significant difference was found in individual ethical profile between Spain (the highest at 3.75) and the USA (the lowest at 3.20, p < 0.01). None of the associative ethical profiles were different between the three countries, although for each country the associative ethical profiles were greater than the individual ethical profiles, a finding we discuss in our discussion section. In light of this result, we focused further analysis on the individual ethical profile only.

<table>
<thead>
<tr>
<th>Country</th>
<th>Individual Ethical Profile Mean (Standard Deviation)</th>
<th>Associative Ethical Profile Mean (Standard Deviation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>3.20 (2.01)</td>
<td>4.28 (1.90)</td>
</tr>
<tr>
<td>Spain</td>
<td>3.75 (1.92)</td>
<td>4.46 (1.86)</td>
</tr>
<tr>
<td>Portugal</td>
<td>3.55 (2.09)</td>
<td>4.33 (2.04)</td>
</tr>
<tr>
<td>Entire Sample</td>
<td>3.44 (2.04)</td>
<td>4.35 (1.90)</td>
</tr>
</tbody>
</table>

Table 2: Individual Ethical Profile and Associative Ethical Profile by Country

We found a high correlation between gender and individual ethical profile. Paired t-tests comparing personal ethical profile for the entire sample and by country consistently indicated men had significantly higher profile scores than women in each of the countries studied. Age and computer knowledge were also factors. Simple regression of age and computer knowledge on personal ethical profile resulted in significant coefficients for both at the p < 0.01 level for the whole sample, although the coefficient for age was negative. This indicated that overall, older respondents reported less incidents of unethical behavior, and those with greater computer knowledge reported more incidents of unethical behavior.

Country-wise comparisons of the individual ethical profile questions using paired t-tests indicate a number of significant differences (all at the p<0.01 or p<0.001 level). For question E3, respondents from Spain and Portugal were significantly more likely to have changed data than were respondents in the USA. For question E4, again respondents from Spain and Portugal were significantly more likely to have used software illegally than were US respondents, but other comparisons were not significant. The most telling difference was with question E5 concerning giving unauthorized access to a computer. Respondents from Spain were much more likely to give unauthorized access than respondents from the other two countries. Respondents from Portugal were significantly more likely to make an illegal copy of software (question E7) than USA respondents. Finally, respondents from the USA and Spain were significantly more likely to download songs without paying than were respondents from Portugal.
Next, we examined responses to the 22 scenario questions. Table 3 lists a summary of the scenario questions and the mean response by country (and for the entire sample) for each question. For each scenario type we ran countrywise comparisons on the questions to identify significant differences. As Table 5 shows, for the “Data Access” scenarios there were numerous significant differences between the three countries respondents (again, highlighted in gray), but no clear trends. Respondents from the USA thought that reading employee email and monitoring web traffic was more acceptable than did respondents in other countries, but conversely they thought someone illicitly accessing source code was clearly unethical while other respondents found it more a questionable activity. For the “Data Manipulation” scenarios, there were only two significant differences. Respondents from Spain found that changing data was more acceptable than did other respondents, while respondents from Portugal found misusing seals of authenticity on a website was less acceptable.

<table>
<thead>
<tr>
<th>Scenario Questions by Scenario Type</th>
<th>Response (mean)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>USA</td>
</tr>
<tr>
<td><strong>Data Access</strong></td>
<td></td>
</tr>
<tr>
<td>Q1a: Email W/Policy (Manager)</td>
<td>2.24</td>
</tr>
<tr>
<td>Q1b: Email W/Policy (Employee)</td>
<td>2.95</td>
</tr>
<tr>
<td>Q10a: Email No Policy (Employee)</td>
<td>3.45</td>
</tr>
<tr>
<td>Q10b: Email No Policy (Manager)</td>
<td>3.02</td>
</tr>
<tr>
<td>Q14: Access of Payroll Records</td>
<td>3.75</td>
</tr>
<tr>
<td>Q18a: Web Traffic Monitoring (Manager)</td>
<td>2.51</td>
</tr>
<tr>
<td>Q18b: Web Traffic Monitoring (Employee)</td>
<td>3.60</td>
</tr>
<tr>
<td>Q21a: Accessing Source Code (Outsider)</td>
<td>4.14</td>
</tr>
<tr>
<td>Q21b: Accessing Source Code (Insider)</td>
<td>4.16</td>
</tr>
<tr>
<td><strong>Data Manipulation</strong></td>
<td></td>
</tr>
<tr>
<td>Q2: Own Data to Avoid Payment</td>
<td>3.72</td>
</tr>
<tr>
<td>Q5: Data Others Utilized</td>
<td>3.98</td>
</tr>
<tr>
<td>Q20: Misrepresent Seals of Authenticity</td>
<td>4.52</td>
</tr>
<tr>
<td><strong>Software Use</strong></td>
<td></td>
</tr>
<tr>
<td>Q3: Does Not Register Software</td>
<td>3.72</td>
</tr>
<tr>
<td>Q4: Gives Old Version of Program to Another Person</td>
<td>3.20</td>
</tr>
<tr>
<td>Q6: Copies Software for Backup Only</td>
<td>2.53</td>
</tr>
<tr>
<td>Q12: Loads Program Onto Two Computers</td>
<td>2.95</td>
</tr>
<tr>
<td>Q22a: Download from P2P Network</td>
<td>3.45</td>
</tr>
<tr>
<td>Q22b: Making DVD of Pirated Music</td>
<td>3.62</td>
</tr>
<tr>
<td>Q22c: Selling DVD of Pirated Music</td>
<td>4.35</td>
</tr>
<tr>
<td><strong>Programming Abuse</strong></td>
<td></td>
</tr>
<tr>
<td>Q8: Non-destructive Virus</td>
<td>3.26</td>
</tr>
<tr>
<td>Q9a: Write Program w/ Inaccurate Data (Programmer)</td>
<td>3.48</td>
</tr>
<tr>
<td>Q9b: Write Program w/ Inaccurate Data (Manager)</td>
<td>4.23</td>
</tr>
<tr>
<td>Q11: Failure to Report Error in Program</td>
<td>3.97</td>
</tr>
<tr>
<td>Q13: Destructive Virus</td>
<td>4.33</td>
</tr>
<tr>
<td>Q17: Spam Database</td>
<td>3.72</td>
</tr>
<tr>
<td><strong>Hardware Use</strong></td>
<td></td>
</tr>
<tr>
<td>Q7a: Gives Access to Account (Account Holder)</td>
<td>3.34</td>
</tr>
<tr>
<td>Q7b: Receives Access to Account (Unauthorized)</td>
<td>3.57</td>
</tr>
<tr>
<td>Q15: Work Computer for Private Business</td>
<td>3.47</td>
</tr>
<tr>
<td>Q16: Creation of Potentially Illegal Database</td>
<td>2.92</td>
</tr>
<tr>
<td>Q19: Use of Computer for Illegal Gambling</td>
<td>3.31</td>
</tr>
</tbody>
</table>

Table 3: Scenario question responses (means) by country (significant differences highlighted in grey)

For the “Software Use” scenarios, we found that respondents from Spain rated questions 4 and 22b more acceptable than others. Respondents from Portugal, however, rated scenarios 6, 12, and 22c as less acceptable than the other countries. In the area of Programming Abuse, respondents from Spain found releasing a non-destructive virus as more acceptable than others but thought that failure to report an error in a program was less acceptable. Conversely, respondents from Portugal rated writing a program to generate inaccurate information as more acceptable than others.
Finally in the area of “Hardware Use,” USA respondents found illegal online gambling from work and setting up an illegal law enforcement database as more acceptable than other countries.

We postulated that individuals’ ethical propensity (represented by their individual ethical profile) would be correlated with their responses to the scenario questions, but we were unsure if and how that relationship would differ depending on the individual’s country of origin. Therefore we correlated individual ethical profile with each of the scenario questions, for each country, using SPSS. We found significant negative correlations (at the p<0.05 level or better) between personal ethical profile and 10 scenario questions for USA respondents; 10 scenario questions for Spain respondents; and 6 scenario questions for Portugal respondents. For each country this was less than half of the scenario questions, which indicates that respondents own experiences may not always influence their ethical attitudes toward other situations.

Finally, we determined if the background differences might provide an alternative explanation for the scenario results by correlating these factors with the scenario questions (first for the entire sample and then for each country). Correlations between background factors and the scenario questions were largely insignificant, and the few significant correlations were low (the highest was a correlation of 0.197, p < 0.01 between scenario question S22c and Age). Since we had identified significant differences in these factors by country we then proceeded to correlate the responses for each country. For each of the three countries, correlations mirrored the entire sample correlations and were significant but low (<0.3), or insignificant, with a few exceptions. Specifically, we found that for Portugal four responses were correlated with age, six responses were correlated with year in school and two with computer knowledge, however correlations in each case were low to modest (0.2 – 0.4 range). These factors (age, year in school and computer knowledge for Portugal) were not significantly higher or lower than the average compared to the other countries based on our earlier analysis. Therefore we concluded that there were no systematic influences of these background factors on the scenario and ethical profile questions.

DISCUSSION

We were able to draw a number of interesting conclusions from our results. First, although we found a few significant differences in the background of our respondents from different countries (such as the greater percentage of female respondents from Spain and less advanced year in school for Spain), we do not believe that these factors systematically influenced respondents ethical profiles or scenario responses by country. Consistent with prior research (Harris, 2000) however, we did find that men universally had higher personal ethical profile scores than women, indicating greater experience with unethical or illegal activities. We expected the negative relationship between age and ethical profile (since older students would have more exposure to consequences of unethical/illegal actions) and the positive relationship between computer knowledge and ethical profile (since more knowledgeable respondents would have more personal opportunity to engage in unethical computer behavior). However we anticipated these factors would also be universally influential, but they were not. This result is possibly related to the age at which respondents first obtain access to computer technology, which might be country specific as it relates to family norms or the educational system. Unfortunately we do not have access to this data, so we can only speculate as to this discrepancy.

We expected that individual ethical profile would tell us something about the differences between the three countries, but unexpectedly our composite scores for both individual and associative ethical profile were very similar across the countries. As expected, associative ethical profiles were greater than individual profiles for each country, likely due to one of two factors. First, respondents may have been more hesitant to answer affirmatively regarding their own illicit behaviors but were perhaps less reluctant when discussing the behavior of their peers. Thus a type of social desirability bias may account for the difference. However since the survey was anonymous it is more likely that the associative profiles are higher because respondents drew on their knowledge of several peers and that as a group the peers’ illicit experiences were more frequent than the respondent’s alone.

When we analyzed the individual ethical profile questions individually we found the incidence of unethical behavior varied greatly depending on the question, since some represented unethical behavior while others represented illegal behavior. Looking overall at the thirty scenario questions, in seven of the questions, all of the countries means were statistically equal. USA had the fewest questions with significant differences (4), although their number was only one less than Portugal. In looking at the data by country, the USA had significant differences in only two scenario types, “Data Access” and “Hardware Use.” No two countries had significant differences in the same two scenario types.
Several interesting observations occurred when we looked at each of the scenario types as a group. Looking at the “Data Access” scenarios, the USA had the least tolerance (highest mean score) with three of the scenarios and the highest tolerance (lowest mean score) with three of the questions. Spain had the least tolerance (highest mean score) with two of the scenarios and the highest tolerance (lowest mean score) with three of the questions. Finally, Portugal had the least tolerance (highest mean score) with three of the scenarios and the highest tolerance (lowest mean score) with two of the questions. Although there were differences, no clear patterns emerged from the data in this area. The “Data Manipulation” scenarios results were also spread among the countries with no clear pattern emerging from the data.

In the “Software Use” scenario type, Spain had the most tolerance (lowest mean score) for all seven scenarios. Portugal had the highest mean score in four of the scenarios, with the US had the highest mean score in the other three scenarios. No obvious cultural distinctions that we know if could account for these results, especially when compared with Portugal. We are working with colleagues in those two countries to try and explain this seemingly anomaly.

In the “Programming Abuse” scenarios, the USA had the least tolerance (highest mean score) in two of the scenarios, Portugal had the highest mean scored on three scenarios and Spain had the highest mean score on one scenario.. The highest tolerance (lowest mean score) was similarly divided. Finally, in the “Hardware Abuse” category, Portugal had the lowest tolerance (highest mean score) on four of the five scenarios. The highest tolerance (lowest mean score) scores were split between the USA (three) and Spain (two).

Overall, Portugal had the least tolerance (highest mean score) in thirteen of the scenarios to lead all countries. They had the highest tolerance (lowest mean score) in only five of the scenario. A possible explanation is Portugal’s extremely high score in Hofstede’s Uncertainty Avoidance dimension (see Table 1). Given this unusually high score (it was the second highest of all countries with an Uncertainty Avoidance score) the Portuguese do not like uncertainty. They tend to plan everything carefully and try to avoid risk. In Portugal, the culture relies on rules, laws and regulations. This might explain the low tolerance for unethical or illegal activities. The USA, on the other hand, had the least tolerance (highest mean score) in nine of the scenarios and the highest tolerance (lowest mean score) for nine of the scenarios. The USA had the highest score of any of the countries in the study in Hofstede’s Individualism dimension. This individualism might explain why they had an equal number of high and low mean scores. Finally, Spain had the least tolerance (highest mean score) in nine of the scenarios and the highest tolerance (lowest mean score) for sixteen of the scenarios, considerably higher than any other country. Maybe it was a combination of age (Spain had the oldest population) and computer knowledge (Spain had the highest computer knowledge). These made Spanish respondents more sensitive to computer ethics and less likely to tolerate computer abuses. Again, we are working with colleagues in Spain to try and explain these results.

CONCLUSION

We are becoming a global economy. Companies are connected with each other via global trade, information and communication technologies, products/services that span countries and cultures, and keen interests of knowing and working with others who live around the world. Information is particularly important for the successful operations of an NMC. The geographical nature of business creates differences in culture, expectations, business norms, educational systems, legal systems, and ethical values in the global economy. It is vital for multinational organizations to understand these differences to understand the actions of their employees regarding ethical actions.

In this paper, we have taken a critical look at how culture may impact the actions of individuals in organizations that cross country boundaries by looking at ethical attitudes and behaviors. The three countries studied yielded interesting differences in how ethical attitudes and behaviors are manifested with respect to sensitive information assurance and security areas.

REFERENCES