Online Journal of Applied Knowledge Management
A Publication of the International Institute for Applied Knowledge Management
Volume3, Issue 2, 2015

Pharmaceutical companies' documented and online privacy practices: Development of an index measure and initial test

Shonda D. Brown, *Nova Southeastern University, bshonda@nova.edu*
Yair Levy, *Nova Southeastern University, levyy@nova.edu*
Michelle M. Ramim, *Hodges University, mramim@hodges.edu*
James L. Parrish, *Nova Southeastern University, jlparrish@nova.edu*

Abstract

Consumers have begun to take a more proactive approach to their healthcare by accessing pharmaceutical companies Websites to obtain health and drug information. In exchange for these benefits, companies require consumers to voluntarily disclose information. However, research has shown that consumers continue to be concerned about how their information is managed, used, and distributed by companies, especially if accessed via the Web. To date, there has been limited empirical research to examine the actual online practices of companies when it comes to privacy, especially those of pharmaceutical companies. Using the Delphi expert panel process, we identified the components of a hierarchical benchmarking index to examine the documented and actual online practices of 100 Website registrations with pharmaceutical companies. In this paper, we outline the development of an index to measure the personal information privacy violations of pharmaceutical companies using hierarchical linear technique. Second, we provided empirical evidence regarding the magnitude of voluntary adherence to the Fair Information Practices (FIPs) by pharmaceutical companies based upon the personal information privacy violations. Our results revealed that companies with headquarters in Europe had fewer personal information privacy violations than those in the US. Moreover, our results indicate that fewer personal information privacy violations occur for chronic conditions than for non-chronic conditions, as well as fewer violations occur with Website registrations for updates than for discounts. Finally, both Europe and UK demonstrated more overall adherence to the FIPs than the US and Asia. This suggests that self-regulation may not be sufficient, while more enforcement may be necessary to decrease personal information privacy violations.

Keywords: *Personal information privacy violations; Consumer control; Fair information practices; Information privacy; Information sharing; Pharmaceutical companies' online practices; Hierarchical privacy index development*

Introduction

The technological advancement of the Internet has revolutionized the way companies interact with consumers by enabling the ability to collect, store, transfer, sell, and analyze consumer

information (Lanier & Saini, 2008; Rapp, Hill, Gaines, & Wilson, 2009; Xu, 2009). Companies are able to leverage the Internet to establish relationships with consumers through the selling of products and services or to be a source of information. However, in order to establish this relationship and engage in target marketing, companies must collect information either by voluntary or involuntary methods (Christiansen, 2011). According to Christiansen (2011), "a user's voluntary sharing of such information" (p. 509) is considered voluntary disclosure and one of the methods of collecting information. Christiansen (2011) also noted that involuntary methods are malicious and "involve the use of technology to collect data and track movements by Internet users without their knowledge and/or permission" (p. 511). Once the information is collected, the storage, access, and distribution are managed by the company (Milne, Rohm, & Bahl, 2004). As a result, the information becomes at risk for secondary use, unauthorized access, and sharing with third parties (Milne et al., 2004). Hoffman, Novak, and Peralta (1999) defined secondary use as "the use of personal information for other purposes, subsequent to the transaction where the information was originally collected" (p. 131). In the same context, Culnan and Armstrong (1999) defined information sharing as "sharing personal information with others who were not a party to the original transaction" (p. 106). With the increase use of Web-based systems, companies' online practices of information sharing (OPIS) are proliferating, and so does risks related to the privacy of such information. Because of the information sharing risks by companies, the online practices of consumer control (OPCC) are important to consumers (Liu, Marchewka, Lu, & Yu, 2005). Hoffman et al. (1999) defined consumer control as "the consumer's ability to control the dissemination of information related to or provided during such transactions or behaviors to those who were not present" (p. 131). Liu et al. (2005) further noted that consumers expect to maintain some level of control over how their information is used and distributed.

Because of the aforementioned risks, consumers are exposed to threats, such as identity theft and unsolicited marketing, which contribute to an elevation of consumer personal information privacy concerns (Zorotheos & Kafeza, 2009). As a result, consumers are hesitant to provide personal information via the Internet (Nam, Song, Lee, & Park, 2006). Likewise, Lanier and Saini (2008) noted that, while consumers appreciate the convenience and benefits of various technological advancements, they are concerned about how information collection practices impact their privacy. Therefore, some consumers take prudent actions such as decreasing Internet use, fabricating or falsifying information, and refusing to disclose information (Cromer, 2010; Yang & Wang, 2009). In this respect, Meinert, Peterson, Criswell, and Crossland (2006) noted that e-commerce suffered an approximate $15 billion in unrealized revenue due to lack of consumer trust regarding companies' ability to protect or use their personal information in an ethical manner. In an effort to alleviate consumer concerns, companies post privacy seals and privacy policies on their Website to provide awareness of their information handling practices (Pollach, 2007). Jafarr and Abdullat (2009) defined the documented practices of the privacy policy (DPPP) as a "written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business" (p. 126). Regardless of privacy seals and DPPP, consumers expect companies to have an ethical responsibility to engage in practices that maintain information integrity and protect consumer information from unauthorized disclosure, access,

use, or loss (Peltier, Milne, & Phelps, 2009). Moreover, this expectation is heightened for financial, medical, and health information (Gupta, Iyer, & Weisskirch, 2010; Yang & Wang, 2009). Therefore, given the significant rise in the use of healthcare Websites (Davis, 2012; Kim & King, 2009) and the sensitivity of information, pharmaceutical companies' Websites, the focus of this research study is to investigate the documented and actual online practices that are contributing to the proliferation of online privacy violations by pharmaceutical companies.

In this paper, we outline our research study that developed a hierarchical benchmarking instrument to assess the documented and actual online practices implemented by pharmaceutical companies' Websites. Using hierarchical linear technique of multiple measures, we derived a single composite index that represents an assessment of personal information privacy violations. The Personal Information Privacy Violations Index (PIPVI) hierarchical benchmarking instrument was used to compare the practices implemented from 100 Website registrations of pharmaceutical companies that market prescription medication for chronic and non-chronic conditions. We have selected these two sub-categories of the pharmaceutical market, as both appear to have a significant market share and appear to collect personal information, which a breach of such personal information can cause substantial embarrassment or even harm to individuals. For example, revealing the names of elected official who is taking some mental or other disorder medications can certainly be harmful for their reputation to remain in office. Thus, the main research problem that this study addressed is the proliferation of online privacy violations by companies (Anton, Earp, & Young, 2010; Li, Sarathy, & Xu, 2011; Nam et al., 2006; Peltier et al., 2009).

Theoretical Background

The key theoretical foundation for this research study draws on the social exchange theory (SET). The context of the SET is that there is a voluntary exchange between multiple parties. Homans (1958) noted that "persons that give much to others try to get much from them, and persons that get much from others are under pressure to give much to them" (p. 606). The SET posits that consumers engage in a "privacy calculus" where they assess information disclosure against the expected benefits (Emerson, 1976). During the assessment, consumers evaluate if their information will be used ethically and if they will not suffer negative consequences from information disclosure (Xu, 2009). Yang and Wang (2009) used the SET to examine cost-benefit effects on privacy concern and behavioral intention. They found that privacy concern has a negative effect on information disclosure but a positive effect on privacy intention. In order to make an informed decision, the consumer should have prior knowledge of companies' information practices (Xu, 2009).

According to Westin (1967), information privacy is defined as "the right of individuals, groups, or institutions, to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7). Jafar and Abdullat (2009) noted that "the personal information privacy of an individual is violated when electronic personal information that was entrusted to third parties is electronically shared or crossed referenced with other parties without the consent of the individual" (p. 126). Specifically, consumers continue to be concerned with unsolicited email, identity theft, and negligent information loss through the selling and

unauthorized use of their information when using the Internet (Anton et al., 2010; Lanier & Saini, 2008; Pollach, 2007). Therefore, prior to disclosing information consumers engage in a risk-benefit analysis to evaluate if the benefit of the transaction surpasses the risk of information disclosure (Xu, 2009; Yang & Wang, 2009). This behavior is consistent with the value and stimulus propositions of the Social Exchange Theory (SET). The value proposition noted that "the more valuable to a person is the result of his action, the more likely he is to perform the action" (Emerson, 1976, p. 340). The stimulus proposition noted that:

> If in the past the occurrence of a particular stimulus, or set of stimuli, has been the occasion on which a person's action has been rewarded, then the more similar the present stimuli are to the past ones, the more likely the person is to perform the action, or some similar action now. (Emerson, 1976, p. 339)

In other words, Emerson (1976) noted that if consumers perceive that the expected benefit prevails over the risk of information disclosure, they would voluntarily disclose the information. Likewise, if consumers have previously disclosed information and received the reward without perceptions of personal information privacy violation, they will be more willing to disclose information in similar conditions (Emerson, 1976). However, Nam et al. (2006) noted that "media scrutiny of Internet fraud, hacking, and identity theft has heightened people's awareness of the risks of conducting transactions on the Internet" (p. 212).

Identity theft and other personal information privacy violations in the United States (US) have continued to rise and receive media attention. For instance, Federal Trade Commission (FTC) (2013) reported that in 2012 identity theft was the top consumer complaint with 369,212 incidents. The Privacy Rights Clearinghouse (2013) reported that since 2005 there have been 932,729,111 records breached containing personal information from 4,478 reported incidents. Meanwhile, the Internet Crime Complaint Center (IC^3) (2014) noted that over three million incidents have been reported since 2000. It is important to note that IC^3 reported that the first million complaints occurred over seven years with the next million occurring in 3.5 years, indicating a significant escalation in cyber crimes each year. The IC^3 (2010) indicated that a substantial number of complaints are due to loss of personally identifiable information (PII). Culnan and Armstrong (1999) defined PII as "information identifiable to an individual" (p. 105). The aforementioned incidents are significant indicators of the growth and occurrence of personal information privacy violations occurring through the use of the Internet and are key contributors to the escalation of consumer concerns (Lanier & Saini, 2008; Zorotheos & Kafeza, 2009).

In response to the reoccurrence of personal information breaches in the US, the FTC established or adopted laws and regulations to protect consumers. The Fair Information Practices (FIPs) are "global principles that fairly balance the need for business to collect and use personal information with the legitimate privacy interests of consumers to be able to exercise control over the disclosure and subsequent uses of their personal information" (Milne & Culnan, 2002, p. 345). FIPs are generally contained in a Website's DPPP. However, enforcement of the FIPs occurs through self-regulation (Lanier & Saini, 2008; Nemati & Dyke, 2009; Xu, 2009). According to Xu (2009), "self-regulation involves the setting of standards by an industry group

or certifying agency and the voluntary adherence to the set of standards by members or associates" (p. 24). In other words, companies are responsible for voluntarily compliance with these laws and regulations (Nemati & Dyke, 2009). Despite the existence of a Website's DPPP and other US laws and regulations, the FTC (2013) noted that it continues to address cases of personal information privacy violations in the US with multi-million dollar settlements.

Although consumer concerns are increasingly rising, so does Internet use, which implies that consumers are being more meticulous about interaction with particular Websites (Cromer, 2010). For instance, Nam et al. (2006) noted that the use of the Internet as an informational source has surpassed the purchasing of products. In this respect, as consumers begin to take a more proactive approach to their healthcare, the use of the Internet to obtain medical drug information is also on the rise (Davis, 2012). Davis (2012) indicated that the Internet is the second most used source for prescription drug information after healthcare physicians. However, Davis (2012) further noted that consumers prefer pharmaceutical companies' Websites as a primary source of information. Kim and King (2009) noted that consumer's access of pharmaceutical companies' Websites tripled from 2000 to 2003. This proliferation is supported by Joseph, Spake, and Finney (2008) who also noted that less than 10% of consumers indicated physicians should be the primary source for pharmaceutical information. This is evident by consumer use of pharmaceutical companies' Websites to access health and drug information, support groups, free drug samples, and rebates (Sheehan, 2005). It is important to note that to acquire those benefits consumers are required to disclose personal information. Equally important, consumers are more cautious about disclosing personal information with health Websites due to the sensitivity of information that may be required and the risk of companies developing inferences using information collected. For example, Bansal, Zahedi, and Gefen (2010) noted that personal health information could be used by employers or insurance agencies to discriminate against consumers. Therefore, it is important for consumers to understand the documented and actual online practices of any company they interact with (Milne, Rohm, & Bahl, 2004; Van Dyke, 2007). Thus, additional research of the online information practices of Websites is warranted to understand the practices that are contributing to the proliferation of online privacy violations by companies (Lanier & Saini, 2008).

Research Questions and Hypotheses

Our main goal in this research study was to develop the Personal Information Privacy Violation Index (PIPVI) benchmarking instrument based on a hierarchical composition of the documented practices of the privacy policy measure (DPPPM), online practices of information sharing measure (OPISM), and the online practices of consumer control measure (OPCCM) to derive the PIPVI. Davis (2012) noted that consumers use the Internet as source for medical information in addition to their physician. Kim and King (2009) also asserted that "Internet sources are more important for prescription drugs than for non-prescription drugs" (p. 5). Based upon the growth projections for the chronic and non-chronic prescription medication markets, it is expected that consumer use of pharmaceutical Websites will continue to rise. Therefore, it is important to understand the documented and actual online information practices of pharmaceutical companies to gain insight into how they use the information collected through their Websites. Our

expectation was that with the use of actual counting of violations, as opposed to perception-based survey, our research study provides insight into the practices that are contributing to PIPV. Given the heightened concerns of consumers regarding personal information privacy, the results of this research study provides consumers with empirical evidence of how information is managed and used by pharmaceutical companies. Consumers will be able to assess the magnitude of information sharing and ability (or lack thereof) to control their information. A high magnitude of personal information privacy violations could negatively impact consumers' trust, concerns, and interactions with the Websites, which could continue to constrain the growth of e-commerce. Because enforcement of the FIPs occurs through self-regulation, the results of this research study provide evidence regarding the magnitude of voluntary adherence to the FIPs by pharmaceutical companies. This evidence can assist advocacy groups and regulators with understanding the effectiveness of self-regulation. Furthermore, it can aide in determining if more stringent laws and regulations or enforcement is necessary. In addition, companies can use the PIPVI benchmarking instrument to perform a self-assessment of their Website documented and online practices, while seeing how these differ or change over time.

We have set eight research questions and three hypotheses for this research study. Figure 1 represents the conceptual model for the PIPVI.

RQ1a: What are the experts' approved components of the DPPP implemented by pharmaceutical companies using a Delphi expert methodology?

RQ1b: What are the experts' approved weights of the DPPP's components implemented by pharmaceutical companies using a Delphi expert methodology?

RQ2a: What are the experts' approved components of the OPIS implemented by pharmaceutical companies using a Delphi expert methodology?

RQ2b: What are the experts' approved weights of the OPIS's components implemented by pharmaceutical companies using a Delphi expert methodology?

RQ3a: What are the experts' approved components of the OPCC implemented by pharmaceutical companies using a Delphi expert methodology?

RQ3b: What are the experts' approved weights of the OPCC's components implemented by pharmaceutical companies using a Delphi expert methodology?

RQ4: What are the experts' approved weights of the single, integrated, hierarchical measure of PIPVI's components of DPPP, OPIS, and the OPCC implemented by pharmaceutical companies using a Delphi expert methodology?

RQ5: Are there any statistical significance mean differences for DPPM between pharmaceutical companies that headquarters are based in United States versus Europe, Asia, or United Kingdom?

RQ6: Are there any statistical significance mean differences for OPISM, OPCCM, and PIPVI between pharmaceutical companies that a) market chronic versus non-chronic prescription medications, b) market registrations for prescription

medication discounts versus updates, c) their headquarters are based in United States, versus Europe, Asia, or United Kingdom?

RQ7: Are there any significant differences between the documented and the actual online practices for choice, and access of pharmaceutical companies that a) market chronic versus non-chronic prescription medications, b) market registrations for prescription medication discounts versus updates, c) their headquarters are based in United States, versus Europe, Asia, or United Kingdom?

RQ8: Are there any statistical significance mean differences for OPISM, OPCCM and PIPVI between pharmaceutical companies that collect a limited amount of PII and those that collect a high amount of PII?

H_1: The pharmaceutical company's DPPPM, OPISM, OPCCM, and PIPVI will not be significantly different when controlling for company size.

H_2: The pharmaceutical company's DPPPM, OPISM, OPCCM, and PIPVI will not be significantly different when controlling for annual revenue.

H_3: The pharmaceutical company's DPPPM, OPISM, OPCCM, and PIPVI will not be significantly different when controlling for years in existence.

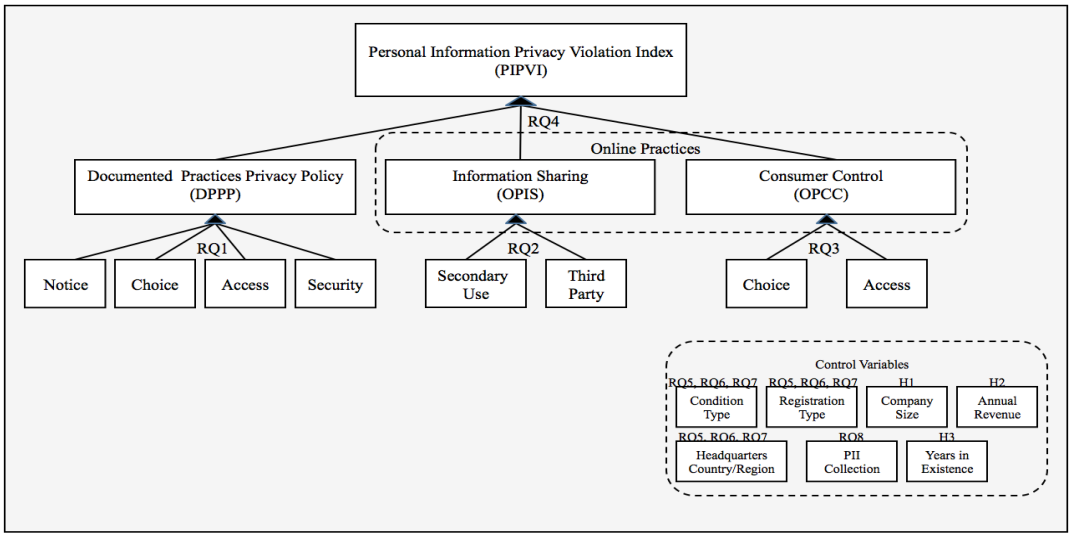

Figure 1: Conceptual Model for Personal Information Violation Index (PIPVI)

Methodology

Our research study developed the PIPVI hierarchical benchmarking instrument that was used to assess the documented and actual online practices using data collected to develop a comparison report based upon 100 Website registrations of 25 pharmaceutical companies that market chronic and non-chronic prescription medications. See Table 1 for pharmaceutical company and Website demographics. Three phases were used to achieve the research goal. The first phase included the development and validation of the PIPVI hierarchical benchmarking instrument using the Delphi expert methodology. Dalkey and Helmer (1963) noted that the Delphi expert methodology's

objective is "to obtain the most reliable consensus of opinion of a group of experts" (p. 458). Sarlak and Aliahmadi (2008) further stated that "the notion is that well informed individuals, calling on their insights and experience, are better equipped to predict the future than theoretical approaches or extrapolation of trends" (p. 1468). The Delphi expert methodology requires recurring elicitation from the expert panel using a questionnaire or interview to eliminate direct disagreement among the expert panel (Dalkey & Helmer, 1963). Ramim and Lichvar (2014) indicated that "the Delphi methodology is mainly used in the situation where accurate information is unavailable and human judgment input is crucial" (p. 127). For our expert panel, at least 35 individuals from academia and practitioners in the fields of information security, privacy, as well as corporate social responsibility was solicited to participate from professional contacts with those associated to this research project as well as membership in professional society mailing lists. The expert panel was requested to evaluate the documented and online practices criteria, as well as assess the relative importance of each criterion in DPPP, OPIS, and OPCC. The relative importance of each criterion within each measure (DPPPM, OPISM, & OPCCM) was combined to develop the PIPVI. After consensus was achieved through several iterations with the expert panel, the feedback was incorporated to create the final PIPVI hierarchical benchmarking instrument based on the weights and validity of the criteria. The second phase used the Delphi-based developed PIPVI benchmarking instrument to assess the documented and actual online practices implemented from 100 Website registrations of pharmaceutical companies that market chronic and non-chronic prescription medications. In addition, the demographic information collected for each pharmaceutical company was used to assess if there are any significant differences in the pharmaceutical company's PIPVI, DPPPM, OPISM, and OPCCM based on its headquarters country/region, company size, annual revenues, condition type (chronic vs. non-chronic), and registration type (discount vs. update). To assess the pharmaceutical company's DPPP, a copy of the privacy policy was downloaded and analyzed against the FIPs. To assess OPIS and OPCC, registration for a newsletter, update, discount, or support program was initiated with a unique name and email address for each Website registration. This enabled an assessment of the types of PII collected, information sharing, consumer choice, and access practices for each pharmaceutical company Website. The use of a unique name and email address for each Website registration maintained data integrity and facilitated accurate descriptive metrics for each. Otherwise, it would have been a potential challenge to determine accurate metrics for the origination of emails to assess information sharing for each pharmaceutical company Website. The third phase was to prepare a comparison report using the data collected in the PIPVI benchmarking instrument from 100 Website registrations of pharmaceutical companies that market chronic and non-chronic prescription medications.

Table 1

Pharmaceutical Company and Website Demographics

				Condition Type		Registration Type	
Headquarters Country/Region	**n**	**%**	**Website Registrations**	**Chronic**	**Non-Chronic**	**Discount**	**Update**
Asia	2	8%	8	6	2	6	2
Europe	6	24%	37	24	13	15	22
United Kingdom	1	4%	5	0	5	3	2
United States	16	64%	50	19	31	24	26
Totals	25	100%	100	49	51	48	52

Instrument Validity and Reliability

According to Creswell (2002), "content validity is the extent to which the questions on the instrument and the scores from the questions are representative of all the possible questions that could be asked about the content or skills" (p. 184). Creswell (2002) defined validity as the researcher's ability to "draw meaningful and justifiable inferences from scores about a sample or population" (p. 185). Sekeran (2003) further noted that "validity ensures the ability of a scale to measure the intended concept" (p. 206). Creswell (2002), Sekeran (2003), and Straub (1989) indicated that a panel of judges or experts could be used to validate the instrument content.

Reliability is important because it indicates the extent of un-bias and is an indication of stability and consistency (Sekeran, 2003). Straub (1989) contended that it is important to show evidence that the instrument is measuring what it intends to measure, i.e. reducing threats to internal validity. McFadzean, Ezlingeard, and Birchall (2011) noted that the Delphi expert methodology "ensures that the data collection process is both reliable and valid because it exposes the investigation to differing, and often divergent, opinions and seeks convergence through structured feedback" (p. 108). Therefore, to ensure both validity and reliability, in this research study, we elicited feedback from the expert panel to verify that the criteria used to generate the measures were appropriate to assess the documented and online practices.

Data Analysis

The data collected was first subjected to pre-analysis data preparation, where it was examined for accuracy in preparation for analysis (Levy, 2006; Mertler & Vannatta, 2010). The first data set from the expert panel was tabulated in the data screening process. Those values were placed into a table with responses from each expert panelist that represents their preference for the DPPP, OPIS, and OPCC criteria and weights. Following the initial data entry tabulation, one more researcher reviewed the records to ensure accuracy. Afterwards the mean was computed for each weight. It is important to note that the combined weights must total 100%, as the focus of the index is to evaluate the distribution of importance across all criteria measured. The second data set from the PIPVI benchmarking instrument was collected from the 100 Website registrations of pharmaceutical companies that market chronic and non-chronic prescription medications. Those

values were placed into a table with responses for each Website registration for the pharmaceutical company. Once observed values were tabulated, they were divided by the total number of criteria for DPPP, and OPCC. For OPIS, the observed values were divided by the maximum number of emails. Afterwards, the values were multiplied by the Delphi expert panel approved weight for each criterion to compute the measures DPPPM, OPISM, and OPCCM. These calculated measures were then multiplied by the expert panel approved weights and combined to derive the hierarchical PIPVI for the sample of registrations for the pharmaceutical company Websites. The calculated PIPVI was used to sort the data and compute the standard deviation (SD), which was used to develop the comparison report to address the research questions and hypothesis (See Eq. 1, 2, 3, & 4). Next, statistical tests, such as factorial analysis of variance (ANOVA) was conducted to further compare the data based upon the pharmaceutical companies condition types (chronic vs. non-chronic), registration types (updates vs. discounts), and headquarters country/region (Asia, Europe, United Kingdom, & United States), which addressed research questions five and six. Additional statistical tests, such as factorial analysis of variance (ANOVA), factorial analysis of covariance (ANCOVA), chi-square, and Spearson correlation were conducted to further compare the data based upon the pharmaceutical company's documented versus actual practices, PII collection, its headquarters country/region, company size, and reported annual revenue to assess any significant differences in the PIPVI. These analyses addressed research questions seven, eight, and all three hypotheses. Figure 2 depicts how the index value was derived from the three measures and the germane criteria for each measure.

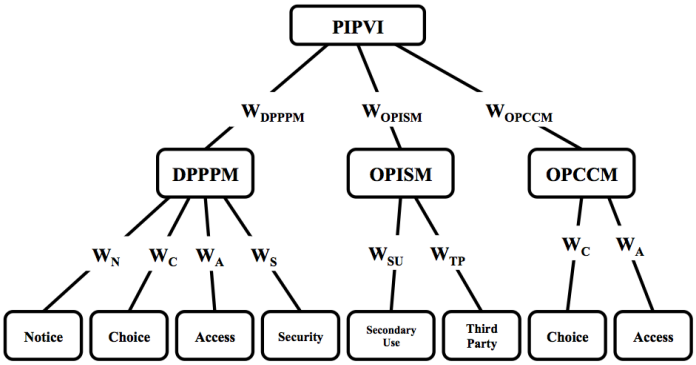

Figure 2: Hierarchical View of the Index, Measures, and Criteria of PIPVI

Eq. 1: $$DPPPM = \left(w_N \cdot \frac{Notice}{Total\ Criteria}\right) + \left(w_C \cdot \frac{Choice}{Total\ Criteria}\right) + \left(w_A \cdot \frac{Access}{Total\ Criteria}\right) + \left(w_S \cdot \frac{Security}{Total\ Criteria}\right)$$

Eq. 2: $$OPISM = \left(w_{SU} \cdot \frac{Secondary\ Use}{Max\ SU\ Emails}\right) + \left(w_{TP} \cdot \frac{Third\ Party}{Max\ TP\ Emails}\right)$$

Eq. 3: $$OPCCM = \left(w_C \cdot \frac{Choice}{Total\ Criteria}\right) + \left(w_A \cdot \frac{Access}{Total\ Criteria}\right)$$

Eq. 4: $$PIPVI = W_{DPPPM} \cdot DPPPM + W_{OPISM} \cdot OPISM + W_{OPCCM} \cdot OPCCM$$

Results

The results for our research study are three folds. First, the research study was conducted with an expert panel using the Delphi Method in early June, 2014 and concluded late September, 2014. The expert panel was solicited by email, and professional society mailing lists. Second, after data collection from the 100 Website registrations, our results revealed if there are statistical mean differences in PIPVI, DPPPM, OPISM, and OPCCM between pharmaceutical companies that market chronic and non-chronic prescription medications. Last, the results revealed if there were any significant differences in the pharmaceutical company's PIPVI, DPPPM, OPISM, and OPCCM based on headquarter country/region, company size, and annual revenues.

To answer the first four research questions, the expert panel participated in two rounds using the Delphi Method. In the first round, the expert panel was solicited to validate that the proposed measures and criteria were sufficient to measure personal information privacy violations, in addition to eliciting the relative weight allocations. An email that contained a link to a Web-based survey tool was used to record the opinions of the expert panel using a survey instrument. Twenty-five participants completed the first survey and no responses were omitted. The expert panel was requested to specify their level of agreement for the measures and criteria based upon on a Likert scale from 1 = strongly disagree to 7 = strongly agree. The level of agreement for at least somewhat agreed (5) or above ranged from 68% to 96%. After assessment of the comments from the expert panel, capturing the volume of phone calls/text messages were added to the criteria for OPIS to assess secondary and third party use. Because the comments were general in nature pertaining to the measures, criteria, and practices, no further additions were warranted.

After the mean was calculated from the relative weights suggested by the expert panel in the first round, the second round of the survey was to elicit responses to validate the relative weights were sufficient for the measures and criteria using a nominal scale with levels: no (0) and yes (1). For this round, 23 participants completed the survey. After tabulation of the survey responses, two responses regarding the weight allocations for DPPPM criterion were omitted for the DPPP because the recommended weight distribution did not total 100%. In this round, the level of agreement for this survey ranged from 48% to 78%. For the level of agreement between 48% and 65%, the suggested mean weights for those that did not agree were within 5% of the proposed weight. Therefore, the proposed weight was determined to be sufficient, and additional rounds were not conducted. See Table 2 for the final weight allocations based upon the expert panel's opinion.

Table 2

PIPVI Criteria, Measures, and Weights Results from the Delphi Expert Panel

DPPP				**OPIS**		**OPCC**		**PIPVI**		
Notice	Choice	Access	Security	Choice	Access	Choice	Access	DPPPM	OPISM	OPCCM
25%	22%	20%	33%	55%	45%	58%	42%	35%	33%	32%
100%				100%		100%		100%		

To examine the fifth research question, differences in the DPPPM scores by headquarters country/region were examined. When the ANOVA was conducted for the DPPPM scores by headquarters country/region, the results were not significant, $F(3, 21) = 1.86$, $p = 0.168$, partial $\eta^2 = 0.21$. This suggests that there were no significant differences in DPPPM scores by headquarters country/region. For the sixth research question, the ANOVAs for OPISM, OPCCM, and PIPVI scores by condition type, registration type, and headquarters country/region were examined. No significant differences were found in the OPISM scores. However, significant differences were found in OPCCM scores by condition type, $F(1, 58) = 5.25$, $p = 0.026$, partial $\eta^2 = 0.08$, suggesting that OPCCM scores for chronic conditions tended to be significantly lower than scores for non-chronic conditions. These scores suggest that consumers appear to have more control over their data for chronic conditions than for non-chronic conditions. No other significant differences were found in the OPCCM scores. Significant differences were found in PIPVI scores by condition type, $F(1, 98) = 11.76$, $p = 0.001$, partial $\eta^2 = 0.11$, suggesting that PIPVI scores for chronic conditions were significantly lower than scores for non-chronic conditions. These scores appear to suggest that fewer personal information privacy violations occur for chronic conditions than for non-chronic conditions. PIPVI scores were also significantly different by registration type, $F(1, 98) = 5.12$, $p = 0.026$, partial $\eta^2 = 0.05$, suggesting that PIPVI scores for discount registration types were significantly higher than update PIPVI scores. These scores appear to suggest that more violations occur with Website registrations for discounts than for updates. Finally, PIPVI scores were significantly different by headquarters country/region, $F(3, 96) = 6.48$, $p < 0.001$, partial $\eta^2 = 0.17$. Post hoc pairwise comparisons showed that European PIPVI scores tended to be significantly lower compared to the US PIPVI scores. These results appear to suggest that European countries might be more responsible with management and use of consumer personal information.

To examine the seventh research question, the chi-square analyses (χ^2) for documented versus actual practices were examined by condition type, registration type, and headquarters country/region. A significant difference between documented versus actual practices for the ability to opt-in/opt-out of secondary use after the initial registration and headquarters country/region was found, $\chi^2(6) = 20.20$, $p = 0.003$. Further examination showed that Europe had a higher level of documented versus actual practices agreement for this criterion than any other headquarters country/region. A significant difference between documented versus actual practices for the ability to opt-in/opt-out of third party use after the initial registration and headquarters country/region was found, $\chi^2(6) = 14.19$, $p = 0.028$. Next, a significant difference between documented versus actual practices for the ability to review personal information and headquarters country/region was found, $\chi^2(6) = 17.84$, $p = 0.007$. However, for opt-in/opt-out of third party use after the initial registration and ability to review personal information, expected values were found to be below 1.00, and, thus, caution should be taken in the interpretation and generalization of the chi-square results. Although significance was found, no large differences between the actual and documented values were found in the chi-square. This suggests that there were slight differences between the documented and actual values for all countries, but no major differences. Results of the chi-squares showed a significant difference between documented versus actual practices for the ability to modify personal information and headquarters country/region, $\chi^2(6) = 20.46$, $p = 0.002$. There were more European pharmaceutical companies

with agreement between documented versus actual practices for the ability to modify personal information. There were fewer US pharmaceutical companies with agreement between documented versus actual practices for the ability to modify personal information than expected. Moreover, there were more violations for documented practices by US pharmaceutical companies for the ability to modify personal information than other countries. Next, the results of the chi-square analysis showed a significant difference between documented versus actual practices for the ability to delete personal information and headquarters country/region, $\chi^2(3) = 9.35$, $p = 0.025$. Because the Asian pharmaceutical companies in our study did not have documented practices for delete or provide the ability to delete personal information, they had more agreement between documented and actual practices for the ability to delete personal information than the other countries. All other chi-square analyses for condition type and registration type were not significant.

To examine the eighth research question, additional ANOVAs were conducted to assess if there were differences in OPISM, OPCCM, and PIPVI by PII (low vs. high). Results of the ANOVA for OPISM by PII collection were not significant, $F(1, 58) = 0.42$, $p = 0.517$, partial $\eta^2 = 0.01$. Results of the ANOVA for OPCCM by PII were also not significant, $F(1, 58) = 0.68$, $p = 0.412$, partial $\eta^2 = 0.01$. Finally, results of the ANOVA for PIPVI by PII collection were not significant, $F(1, 58) = 0.05$, $p = 0.819$, partial $\eta^2 = 0.00$. This suggests that no significant differences were found in OPISM, OPCCM, and PIPVI based upon the level of PII collected.

To examine the three hypotheses, the Spearman correlations, non-parametric measures, were used for the differences between DPPM, OPISM, OPCCM and PIPVI with number of employees, annual revenue, and years in existence. OPISM scores differed significantly negatively to annual revenue and positively to years in existence. These scores suggest that as the annual revenue of the company increased, fewer OPIS violations occurred. Surprisingly, as years in existence increased, the more OPIS violations occurred. For PIPVI, the scores differed significantly negatively to both annual revenue and number of employees. This suggests that as annual revenue and number of employees increased, the PIPVI scores tended to decrease, which insinuates fewer personal information violations. No other significant differences were found. Because of these significant differences, the ANOVAs for OPISM and PIPVI were re-conducted as ANCOVAs to assess if controlling for annual revenue and years in existence affects the outcome of the comparisons. The results of the ANCOVA for OPISM scores by condition type after controlling for annual revenue and years in existence were significant, $F(1, 96) = 5.74$, $p = 0.019$, partial $\eta^2 = 0.06$. This is a change from the original ANOVA conducted, and the mean for chronic conditions was significantly higher than the mean for non-chronic conditions. The results of the ANCOVA for OPISM scores by registration type were not significant, $F(1, 96) = 0.26$, $p = 0.611$, partial $\eta^2 = 0.00$, which is similar to the previous results. The results for the ANCOVA for OPISM scores by headquarters country/region were not significant, $F(3, 94) = 0.24$, $p = 0.865$, partial $\eta^2 = 0.01$, mirroring what was previously found.

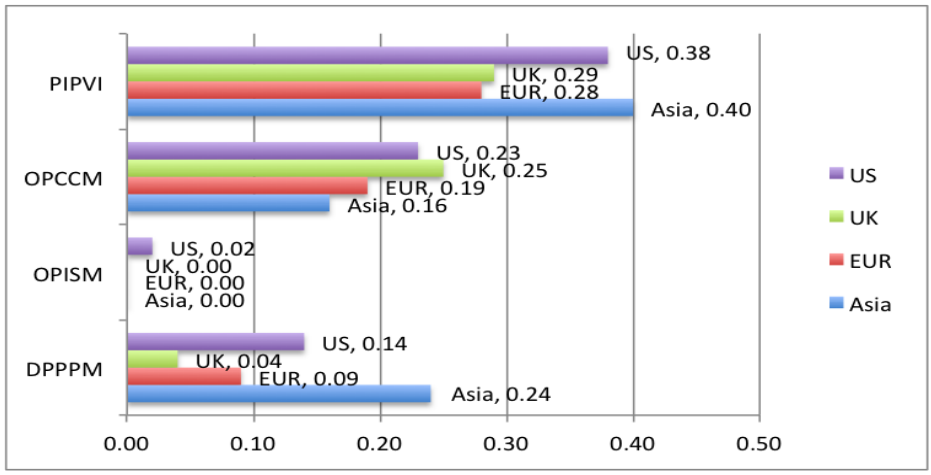

Figure 3: Measures Contributions to PIPVI by Headquarters Country/Region

The results of the ANCOVA for PIPVI scores by condition type while controlling for annual revenue showed significance, $F(1, 97) = 7.79$, $p = 0.006$, partial $\eta^2 = 0.07$, suggesting that the PIPVI scores for chronic conditions were significantly lower than the PIPVI scores for non-chronic conditions. This is similar to the results found in the original ANOVA. Significance was also found by registration type, $F(1, 97) = 4.64$, $p = 0.034$, partial $\eta^2 = 0.05$, also mirroring the results found in the previous ANOVA. Finally, the results for differences by headquarters country/region were also similar to the previous ANOVA, $F(3, 95) = 6.87$, $p < 0.001$, partial $\eta^2 = 0.18$. Thus, from the results of the ANCOVAs, the only change that was made by controlling for the relevant covariates was the ANCOVA for OPISM scores by condition type. Before, the ANOVA results were not significant, but after controlling for registration type and annual revenue, significant differences in OPISM scores were found by condition type. Based upon these results, the null hypotheses two and three were rejected, as a significant difference was found when controlling for annual revenue and years in existence. However, because there was no significant difference found for DPPPM, OPISM, OPCCM, or PIPVI, hypothesis one was accepted. Figure 3 presents the contributions of DPPPM, OPISM, and OPCCM to PIPVI by headquarters country/region.

Discussions and Conclusions

Because incidents continue to rise due to companies' misuse of consumer information (Anton et al., 2010; Lanier & Saini, 2008; Pollach, 2007), our research study attempted to address the proliferation of online privacy violations by companies. We did so by developing a PIPVI benchmarking instrument, including its essential hierarchical components to assess documented and online practices implemented on Websites. This research study achieved the eight research questions and three hypotheses with a three-phased approach. First, an expert panel using the Delphi expert methodology was used to develop the documented practices of the privacy policy measure (DPPPM), online practices of information sharing measure (OPISM), online practices of consumer control measure (OPCCM), and the Personal Information Privacy Violations Index (PIPVI). Second, the PIPVI hierarchical benchmarking instrument was used to assess the documented and online practices implemented from 100 Website registrations of pharmaceutical companies that market chronic and non-chronic prescription medications. Last, a comparison

report was developed for Websites of pharmaceutical companies that market chronic and non-chronic prescription medications.

Overall the results indicated that pharmaceutical companies with headquarters in Europe had fewer personal information privacy violations than the US. In addition, the results suggested that first, as the annual revenue of the company increased, OPIS violations decreased. Second, as years in existence increased, the more OPIS violations occurred. Third, the results suggested that fewer personal information privacy violations occur for chronic conditions than for non-chronic conditions. Third, fewer violations occur with Website registrations for updates than for discounts. Fourth, as annual revenue and number of employees increased, the PIPVI scores tended to decrease, which insinuates fewer personal information violations. Finally, both Europe and UK demonstrated more overall adherence to the FIPs than the US and Asia. This suggests that self-regulation may not be sufficient, while more enforcement may be necessary to decrease personal information privacy violations.

As with any research study, this one also had some limitations. One of the main significant limitations of our study is the generalizable of the specific index values (not the weights) due to the sample used. We expect that the Delphi compositions of the hierarchical weights will be indeed generalized in the future, but as time progresses or the use of the hierarchical benchmarking index on different companies may yield different values. While the sample size of 100 Website registrations is valid, further studies can use a larger sample size to increase validation of the results and generalizability. Next, there was not an equal distribution of pharmaceutical company Website registrations across each headquarters country/region. Furthermore, because some of the Website registrations did not receive any emails, OPIS could not be truly assessed for all pharmaceutical companies Website registrations. Finally, because most pharmaceutical companies noted to submit request for personal information through email, phone, or mail, the delete practices could not be fully assessed.

Recommendations and Future Research

This research study outlined the research plan to develop a set of measures and a single composite index based upon hierarchical criteria identified by current US laws and regulations recommended for ethical business practices for online transactions. The weights of the hierarchical criteria and composite index were developed using a Delphi approach. We then carried out the actual development of the PIPVI, collected, and analyzed the data following the research outline plan discussed here. The findings and the results of the statistical analyses were reported as well. Future studies are warranted to increase the validity of the instrument. In addition, more research will be needed to expand the sample size and the use of other industries to increase the generalizability. While our work concentrated on the pharmaceutical market, future research could include assessing other industries. Moreover, future work can assess the opt-out practices against the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act). An extension of assessing the opt-out practices could include examining the differences based upon the type of request such as Website or email. Another area of future research includes selection of a population with criteria specifically for males and females or age to determine if the documented and online practices of companies differ by

gender or age. Another area of future research includes having an equal distribution of Website registrations across each headquarters country/region. Finally, because the privacy policies stated that requests to delete information must be submitted by phone, email, or mail, future research could include assessing the delete practices by pharmaceutical companies or other industries.

Acknowledgments

We would like to thank the anonymous referees for their careful review and valuable suggestions. We also would like to thank the accepting editor, Dr. Alex Koohang, for his recommendations and constructive comments.

References

Anton, A. I., Earp, J. B., & Young, J. D. (2010). How Internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy, 8*(1), 21-27.

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49,* 138-150.

Christiansen, L. (2011). Personal privacy and Internet marketing: An impossible conflict or a marriage made in heaven? *Business Horizons*, *54*(11), 509-514.

Chordas, L. (2011). The right prescription? *Best's Review*, *112*(8), 64-66.

Creswell, J. W. (2002). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. Upper Saddle River, New Jersey: Merrill Prentice Hall.

Cromer, C. (2010). Understanding Web 2.0's influences on public e-services: A protection motivation perspective. *Innovation: Management, Policy & Practice, 12*(2), 192-205.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organizational Science, 10*(1), 104-115.

Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science, 9*(3), 458-467.

Davis, J. J. (2012). Content analysis of efficacy descriptions on branded pharmaceutical websites. *Journal of Medical Marketing, 12*(4), 211-220.

Earp, J. B., & Baumer, D. (2003). Innovative Web use to learn about consumer behavior and online privacy. *Communications of the ACM, 46*(4), 81-83.

Emerson, R. M. (1976). Social exchange theory. *Annual Review of Sociology, 2*, 335-362.

Federal Trade Commission. (2013). *The Federal Trade Commission (FTC) Mission.* Retrieved on December 1, 2014, from http://www.ftc.gov/system/files/documents/reports/2013-one-page-ftc-performance-snapshot/2013snapshotpar.pdf

Global Industry Analyst, Inc. (2010, February 18). *US allergy drugs market to exceed 14.7 billion by 2015, according to new report by Global Industry Analysts, Inc.* Retrieved on September 20, 2013, from http://www.prweb.com/releases/allergy_drugs_allergens/allergic_rhinitis/prweb3610254.htm

Gupta, B., Iyer, L. S., &Weisskirch, R. S. (2010). Facilitating global e-commerce: A comparison of consumers' willingness to disclose personal information online in the ` and in India. *Journal of Electronic Commerce Research, 11*(1), 41-52.

Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1999). Information privacy in the marketspace: Implications for the commercial uses of anonymity on the Web. *The Information Society, 15*, 129-139.

Homans, G. C. (1958). Social behavior as exchange. *American Journal of Sociology*, *63*(6), 597-606.

Internet Crime Complaint Center. (2014, May 19). *The Internet crime complaint center receives 3 millionth complaint.* Retrieved December 5, 2014, from http://www.ic3.gov/media/2014/140519.aspx

Internet Crime Complaint Center. (2010, November 15). *The Internet crime complaint center hits 2 million.* Retrieved October 14, 2013, from http://www.ic3.gov/media/2010/101115.aspx

Jafar, M. J., & Abdullat, A. (2009). Exploratory analysis of the readability of information privacy statement of the primary social networks. *Journal of Business and Economics Research*, *7*(12), 123-142.

Joseph, M., Spake, D. F., & Finney, D. (2008). Consumer attitudes toward pharmaceutical direct-to-consumer advertising: An empirical study and the role of income. *International Journal of Pharmaceutical and Healthcare Marketing*, *2*(2), 117-133.

Kim, W. J., & King, K.W. (2009). Product category effects on external search for prescription and nonprescription drugs. *Journal of Advertising*, *38*(1), 5-19.

Lanier, C. D., & Saini, A. (2008). Understanding consumer privacy: A review and future directions. *Academy of Marketing Science Review, 12*(2), 1-49.

Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems, 51,* 434-445.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C-S. (2005). Beyond concern–A privacy-trust-behavioral intention model of electronic commerce. *Information and Management, 42,* 289-304.

McFadzean, E., Ezingeard, J-N., & Birchall, D. (2011). Information assurance and corporate strategy: A Delphi study of choices, challenges, and developments for the future. *Information Systems Management, 28,* 102-129.

Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2006). Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations, 4*(1), 1-17.

Mertler, C. A., & Vannatta, R. A. (2010). *Advanced and multivariate statistical methods* (4th ed.). Glendale, CA: Pyrczak.

Milne, G. R., & Culnan, M. J. (2002). Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 U.S. web surveys. *The Information Society, 18,* 345-359.

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *The Journal of Consumer Affairs, 38*(2), 217-232.

Nam, C., Song, C., Lee, E., & Park, C. I. (2006). Consumers' privacy concerns and willingness to provide marketing-related personal information online. *Advances in Consumer Research, 33,* 212-217.

Nemati, H. R., & Dyke, T. V. (2009). Do privacy statements really work? The effect of privacy statements and fair information practices on trust and perceived risk in e-commerce. *International Journal of Security and Privacy, 3*(1), 45-64.

Palmer, E. (2012, September 20). *Bayer takes aim at J & J Evra with new birth control patch*. Retrieved September 22, 2013, from http://www.fiercepharma.com/story/bayer-takes-aim-jjs-evra-new-birth-control-patch/2012-09-20

Peltier, J. W., Milne, G. R., & Phelps, J. E. (2009). Information privacy research: Framework for integrating multiple publics, information channels, and responses. *Journal of Interactive Marketing, 23,* 191-205.

Pollach, I. (2007). What's wrong with online privacy policies? *Communications of the ACM*, *50*(9), 103-108.

Privacy Rights Clearinghouse. (2013). *Chronology of data breaches: Security breaches 2005–present*. Retrieved on December 10, 2014, from http://www.privacyrights.org/data-breach

Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management, 2*(1), 122-136. Retrieved on September 14, 2014, from http://www.iiakm.org/ojakm/articles/2014/volume2_1.php

Rapp, J., Hill, R. P., Gaines, J., & Wilson, R. M. (2009). Advertising and consumer privacy. *Journal of Advertising*, *38*(4), 51-61.

Sarlak, M. A., & Aliahmadi, A. R. (2008). Recognition of factors affecting students trust in virtual universities using Delpi method. *American Journal of Applied Sciences, 5*(11), 1467-1473.

Sekaran, U. (2003). *Research methods for business: A skill building approach* (4th ed.). New York, NY: John Wiley & Sons.

Sheehan, K. B. (2005). In poor health: An assessment of privacy policies at direct-to-consumer websites. *American Marketing Association*, *24*(2), 273-283.

Straub, D. W. (1989) Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-170.

Van Dyke, T. V. (2007). Ignorance is bliss: The effect of increased knowledge on privacy concerns and Internet shopping site personalization preferences. *International Journal of Information Security and Privacy*, *1*(2), 74-92.

Westin, F. (1967). *Privacy and freedom.* New York; Atheneum.

Xu, H. (2009). Consumer responses to the introduction of privacy protection measures. *Journal of E-Business Research*, *5*(2), 21-47.

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *DATA BASE for Advances in Information Systems*, *40*(1), 38-51.

Zorotheos, A., & Kafeza, E. (2009). Users' perception of privacy and their intention to transact online: A study on Greek Internet users. *Direct Marketing, 3*(2), 139-153.

Authors' Biographies

Shonda D. Brown is a manager at a Fortune 500 company. She is a Ph.D. candidate in Information Systems with a concentration in Information Security at Nova Southeastern University. Her research interests include information security and privacy. She has served as a referee research reviewer for an international scientific journal and conference proceeding. Moreover, she received a Bachelor's degree in Information Systems from Howard University and a Master's degree in Information Systems from Drexel University. She is also a member of AIS, IEEE, ACM, and Upsilon Pi Epsilon Honor Society (UPE).

Yair Levy is a Professor of Information Systems and Cybersecurity at the Graduate School of Computer and Information Sciences, Nova Southeastern University and the director of the Center for e-Learning Security Research (CeLSR). During the mid to late 1990s, he assisted NASA to develop e-learning systems. He earned his Bachelor's degree in Aerospace Engineering from the Technion (Israel Institute of Technology). He received his MBA with MIS concentration and Ph.D. in Management Information Systems from Florida International University. His current research interests include security issues with cybersecurity skills and competencies, user-authentication, and privacy issues with Web-based and e-learning systems, as well as Social engineering awareness and cyber threat prevention. His research publications appear in numerous peer-reviewed journals and conference proceedings. Also, Dr. Levy has been serving as a member of conference proceedings committee for numerous scholarly conferences. Moreover, Dr. Levy has been serving as a referee research reviewer for hundreds of national and international scientific outlets. He is a frequent invited keynote speaker at national and international meetings on cybersecurity, IS, and online learning topics. Dr. Levy's teaching interests in the masters level include information systems security, e-commerce, and Web development. His teaching interests in the doctoral level include Information Security Risk Management and Advanced Multivariate Research Methods and Statistics. To find out more about Dr. Levy, please visit his site: http://scis.nova.edu/~levyy/.

Michelle M. Ramim is an Associate Professor at the Fisher School of Technology, Hodges University. She has extensive experience in information technology (IT) consulting. Dr. Ramim directed the development and implementations of several IT projects including promotional and interactive websites for major enterprises such as Debeer (Diamond Trading Company). Her current research interests include ethical issues with IT, information security and crisis management, privacy and legal aspects of computing, as well as ethical decision making. She has published articles in peer-reviewed outlets including journals, conference proceedings, encyclopedias, and an invited chapter. A number of her papers won the 'best paper' award in national and international peer-review conference proceedings. Moreover, she has been serving as a referee research reviewer for national and international scientific journals, conference proceedings, as well as management information systems textbooks. She has developed the supplemental material for the Pearlson and Saunders (2012) 5th ed. book "Managing and Using Information Systems: A Strategic Approach" by Wiley & Sons. She earned her Bachelor's degree from Barry University in Miami, Florida. Dr. Ramim has received her Executive MBA

from Florida International University. She completed her Ph.D. in Information Systems at the Graduate School of Computer and Information Sciences, Nova Southeastern University.

James L. Parrish is an Associate Professor of Information Systems at Nova Southeastern University's Graduate School of Computer and Information Sciences (GSCIS) where he mentors doctoral students and teaches graduate courses in IT strategy, enterprise systems, and cloud computing. He earned his doctorate from the University of Central Florida in 2008 and prior to joining GSCIS was a member of the faculty at the University of Arkansas at Little Rock. In addition to his role at GSCIS, he serves as the Vice President of Student Chapters for the Association of Information Systems, the Vice-Chair of the Partnership for Advancing Computing Education (PACE) and is a member of the board of multiple other organizations in academia and industry. In 2014, he was named as one of the most influential persons in South Florida technology by Techweek. Dr. Parrish has had his research published in multiple peer-reviewed journals and in multiple national and international peer-reviewed conference proceedings. His current research interests are in the areas of knowledge management, design science, socio-technical security exploits, and information systems education.