Online Journal of Applied Knowledge Management
A Publication of the International Institute for Applied Knowledge Management

Volume 1, Issue 1, 2013

Towards a development of an index to measure pharmaceutical companies' online privacy practices

[Research in Progress]

Shonda D. Brown, Nova Southeastern University, bshonda@nova.edu

Yair Levy, Nova Southeastern University, levyy@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, support groups, rebates, coupons, as well as free drug trials. 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, especially those of pharmaceutical companies. This work-in-progress research study will outline a research plan to develop a benchmarking instrument to examine the documented and actual online practices of 100 Websites of pharmaceutical companies. In this paper, we will provide empirical evidence regarding the magnitude of voluntary adherence to the Fair Information Practices by pharmaceutical companies. Second, we will propose the development of an index to measure the personal information privacy violations of pharmaceutical companies. We anticipate that our results can provide consumers with empirical evidence of how their information is managed and used by pharmaceutical companies. 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.

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

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 (Jaisingh, Barron, Mehta, & Chaturvedi, 2008; 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 these risks, consumers are exposed to threats, such as identity theft and unsolicited marketing, which contribute to an elevation of consumer personal information privacy concerns (Federal Trade Commission [FTC], 2000; Zorotheos & Kafeza, 2009). As a result, consumers are hesitant to provide personal information online 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; Poddar, Mosteller, & Ellen, 2009; 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 (Kelly & Rowland, 2000; 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 (Kim & King, 2009) and the sensitivity of information, pharmaceutical companies Websites, the focus of this work-in-progress research study is to investigate the documented and actual online practices that are contributing to the proliferation of online privacy violations by companies.

In this paper, we will outline our work-in-progress research study that attempts to develop a benchmarking instrument to assess the documented and actual online practices implemented by pharmaceutical companies' Websites. Using multiple hierarchical measures, we're proposing to derive a single composite index that represents an assessment of personal information privacy violations (PIPV). The Personal Information Privacy Violations Index (PIPVI) benchmarking instrument will be used to compare the practices implemented on 50 Websites of pharmaceutical companies that market birth control and 50 Websites of pharmaceutical companies that market allergy medications. 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. Thus, the main research problem that this work-in-progress research study attempts to address is the proliferation of online privacy violations by companies (Anton, Earp, & Young, 2010; Li, Sarathy, & Xu, 2011; Nam et al., 2006; Nhan, Kinkade, & Burns, 2009; Peltier et al., 2009).

Theoretical Background

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 (Xie, Teo, & Wan, 2006; 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 (1967) noted that if the consumers perceive that the expected benefit prevails over the risk of information disclosure, they will voluntarily disclose the information. Likewise, if consumers have previously disclosed information and received the reward without perceptions of Personal Information Privacy Violation (PIPV), 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).

The key theoretical foundation for this work-in-progress 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 (Culnan & Armstrong, 1999; 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 (Milne & Rohm, 2000; Xu, 2009).
Identity theft and other PIPV in the United States (U.S.) have continued to rise and receive media attention. For instance, Nemati and Dyke (2009) indicated that in 2003 the Federal Trade Commission (FTC) reported 214,905 incidents of identity theft. More recently, the Privacy Rights Clearinghouse (2011) reported that since 2005 there have been 542,648,022 records breached containing personal information from 2,807 reported incidents. Meanwhile, the Internet Crime Complaint Center (IC^3) (2010) noted that over two 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). PII is represented by information such as name, postal address, email address, phone or fax number, Social Security Number (SSN), or credit card number (FTC, 2000). Similarly, non-PII is defined as **"**information that, taken alone, cannot be used to identify or locate an individual" (FTC, 2000, p. 170). Age, gender, income, and education level are examples of non-PII. The aforementioned incidents are significant indicators of the growth and occurrence of PIPV occurring through the use of the Internet and are key contributors to the escalation of consumer concerns (Lanier & Saini, 2008; Zorotheos & Kafeza, 2009).

The online practices of consumer control (OPCC) are also important to consumers (Liu, Marchewka, Lu, & Yu, 2005). In this context, 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) noted that consumers expect to maintain some level of control over how their information is used and distributed. However, the above incidents give rise to consumer concern regarding the inability to control their information. In fact, Bhuleskar, Sherlekar, and Pandit (2009) reported that 45% of emails represent spam and approximately 14.5 billion spam emails are distributed on a daily basis with consumers receiving an estimated average annual spam of 2,500 emails each.

Given the consistent rise in PIPV over the years, the FTC has made consumer protection a critical aspect of its mission (FTC, n.d). The FTC has the statutory authority and responsibility for prohibiting unfair and deceptive practices by holding companies accountable for privacy practices regarding information collection, use, and security (Earp & Baumer, 2003). In response to the reoccurrence of information breaches in the U.S., 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 (FTC, 2000; 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; Storey, Kane, & Schwaig, 2009). Despite the existence of a Website's DPPP and other U.S. laws and regulations, the FTC (2010) noted that it continues to address cases of PIPV in the U.S. 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 (Kim & King, 2009). 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; Schwaig, Kane, & Storey, 2005).

Research Goals

Our main goal in this work-in-progress research study is to propose the development of 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. We will then, document the process we're intending to undergo to use the PIPVI to compare 50 Websites of pharmaceutical companies that market birth control versus 50 Websites of pharmaceutical companies that market allergy medications. Palmer (2012) noted that contraceptives are an $8 billion annual drug market. In addition, Chordas (2011) stated that "in 2009, more than 90 million prescriptions for contraceptives were dispensed" (p. 64). Likewise, a report by Global Industry Analysts, Inc. (GIA) (2010) noted that consumers experiencing allergies are constantly rising and by 2015 this market is expected to surpass $14.7 billion. Joseph et al. (2008) and Sheehan (2005) 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 birth control and allergy 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. The expectation is that our work-in-progress research study will provide insight into the practices that are contributing to PIPV. Given the heightened concerns of consumers regarding personal information privacy, the results of this work-in-progress research study can provide consumers with empirical evidence of how their information is managed and used by pharmaceutical companies. Consumers will be able to assess the magnitude of information sharing and inability 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 work-in-progress research study will provide evidence regarding the magnitude of voluntary adherence to the FIPs by pharmaceutical companies. This evidence will assist advocacy groups and regulators with understanding the effectiveness of self-regulation to 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 change over time.

We've set seven goals for this study. The first goal is to develop and assess the experts' approved components and weights for the DPPP implemented by pharmaceutical companies using the Delphi expert methodology. The second goal is to develop and assess the experts' approved components and weights for the OPIS implemented by pharmaceutical companies using the Delphi expert methodology. The third goal is to develop and assess the experts' approved components as well as weights for the OPCC implemented by pharmaceutical companies using the Delphi expert methodology. The fourth goal is to develop the components of the single, integrated measure of PIPVI based on the hierarchical composition of DPPP, OPIS, and the OPCC that are implemented by pharmaceutical companies using the Delphi expert methodology. The fifth goal is to assess and compare the PIPVI, DPPPM, OPISM, and OPCCM between 50 Websites of pharmaceutical companies that market birth control versus 50 Websites of pharmaceutical companies that market allergy medications. The sixth goal is to assess and compare the PIPVI, OPISM, and OPCCM between pharmaceutical companies that collect a limited amount of PII and those that collect a high amount of PII. The last and seventh goal is to measure if there are any significant differences in the pharmaceutical company's PIPVI, DPPPM, OPISM, and OPCCM based on its headquarters country, size, and reported annual revenues. Figure 1 represents the hierarchical structure of the PIPVI benchmarking instrument.

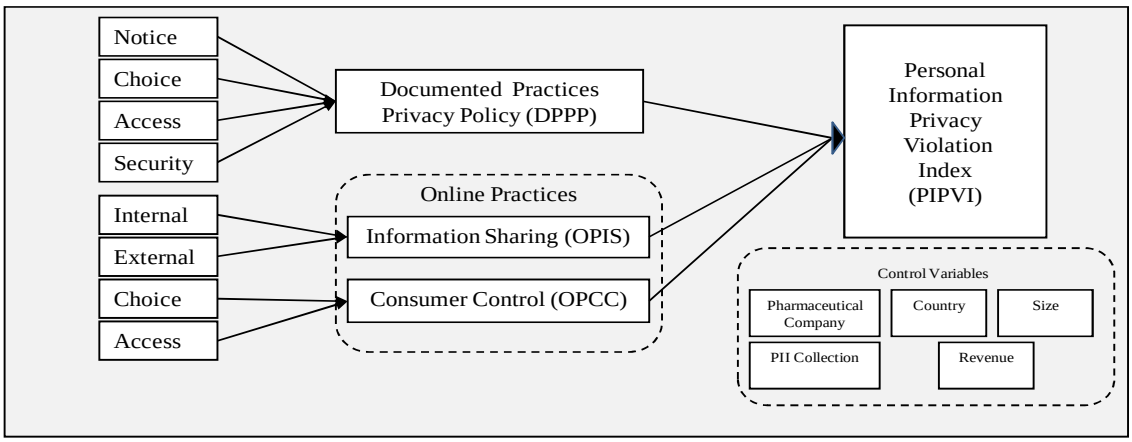

Figure 1: The hierarchical structure of the PIPVI benchmarking instrument

Methodology

Our work-in-progress research study will develop the PIPVI benchmarking instrument that will be used to assess the documented and actual online practices using data collected to develop a comparison report for 50 Websites of pharmaceutical companies that market birth control and 50 Websites of pharmaceutical companies that market allergy medications. Three phases will be used to achieve the work-in-progress research goals. The first phase will include the development and validation of the PIPVI 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). Jain (1985) stated that there should be at least three rounds of elicitation with the expert panel. For this expert panel, at least 35 individuals from academia and practitioners in the field of Information Security and Privacy will be solicited to participate from professional contacts with those associated to this research project and membership in professional societies. The expert panel will be requested to evaluate the documented and online practices, as well as assess the relative importance of each criterion in DPPP, OPIS, and OPCC. The relative importance of each criterion will become the measures (DPPPM, OPISM, & OPCCM) and will be combined to develop the PIPVI. After consensus is achieved through several iterations with the expert panel, the feedback will be incorporated to create the final PIPVI benchmarking instrument. The second phase will use the Delphi-based developed PIPVI benchmarking instrument to assess the documented and actual online practices implemented on 50 Websites of pharmaceutical companies that market birth control and 50 Websites of pharmaceutical companies that market allergy medications. In addition, the demographic information collected for each pharmaceutical company will be used to assess if there are any significant differences in the pharmaceutical company's PIPVI, DPPPM, OPISM,

and OPCCM based on its headquarters' country, size, and annual revenues. To assess the pharmaceutical company's DPPP, a copy of the privacy policy will be downloaded and analyzed against the FIPs. To assess OPIS and OPCC, registration for a newsletter, rebate, discount card, or drug sample will be initiated with a unique name and email address for each Website. This will enable an assessment of the types of PII collected, spam, information sharing, consumer choice, and access practices for each pharmaceutical company. The use of a unique name and email address for each site will maintain data integrity and facilitate accurate descriptive metrics for each pharmaceutical company Website. Otherwise, it would be a potential challenge to determine accurate metrics for the origination of emails to assess spam and information sharing for each pharmaceutical company Website. If the Website's approach is to opt-in for third party or future internal communications, the request will be initiated 10 days after initial registration to assess spam, secondary use of consumer information, and information sharing with third parties before and after the request. The time delay is essential to allow time to assess if spam will be received prior to initiation of opt-in. The third phase will be to prepare a comparison report using the data collected from Websites in the PIPVI benchmarking instrument for 50 Websites of pharmaceutical companies that market birth control and 50 Websites of pharmaceutical companies that market allergy medications.

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 can 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, this work-in-progress research study will elicit feedback from the expert panel to verify that the criteria used to generate the measures are appropriate to assess the documented and online practices.

Data Analysis

The data collected will first be subjected to pre-analysis data preparation, where it will be examined for accuracy in preparation for analysis (Levy, 2006; Mertler & Vannatta, 2010). The first data set from the expert panel will be tabulated in the data screening process. Those values will be placed into a table with responses from each expert panelist that represents their

preference for the DPPP, OPIS, and OPCC weights and the mean will be computed for each weight. It is important to note that the combined weights must total 100%. The second data set from the PIPVI benchmarking instrument will be collected from the Websites of 50 Websites of pharmaceutical companies that market birth control and 50 Websites of pharmaceutical companies that market allergy medications. Those values will be placed into a table with responses for each pharmaceutical company Website. Once observed values are tabulated, they will be multiplied by the Delphi expert panel average weight for each criterion to compute the measures DPPPM, OPISM, and OPCCM. These calculated measures will be multiplied by the average values for the expert panel weights and combined to derive the PIPVI for the sample of pharmaceutical company Websites. The calculated PIPVI will be used to sort the data and compute the standard deviation, which will be used to develop the comparison report to address the proposed research goals (See Eq. 1, 2, 3, & 4). Following, statistical tests, such as factorial analysis of variance (ANOVA) will be conducted to further compare the data based upon the two types of pharmaceutical companies markets (birth control vs. allergy medications), which will address research goal five. Additional statistical tests, such as factorial analysis of variance (ANOVA) and factorial analysis of covariance (ANCOVA), will be conducted to further compare the data based upon the pharmaceutical company's PII collection, its headquarters' country, size, and reported annual revenue to assess any significant differences in the PIPVI. These analyses will address research goals six and seven. Figure 2 depicts how the index value will be derived from the three measures and the germane criteria for each measure.

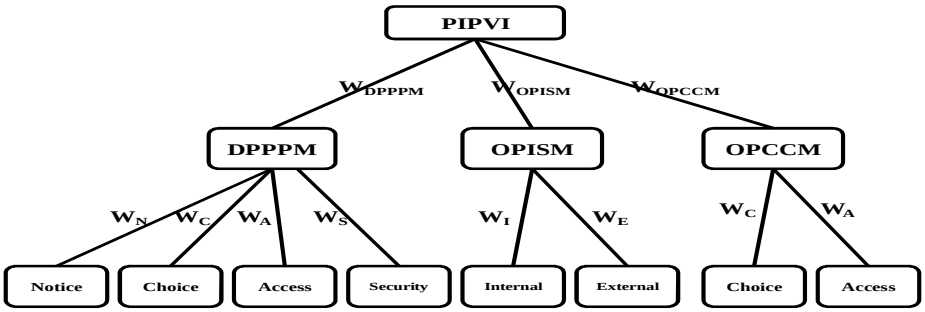

Figure 2: Hierarchical Representation of the PIPVI Benchmarking Instrument, Measures, and Criteria

Eq. 1: $PIPVI = W_{DPPPM} \cdot DPPPM + W_{OPISM} \cdot OPISM + W_{OPCCM} \cdot OPCCM$

Eq. 2: $DPPPM = w_N \cdot Notice + w_C \cdot Choice + w_A \cdot Access + w_S \cdot Security$

Eq. 3: $OPISM = w_I \cdot Internal + w_E \cdot External$

Eq. 4: $OPCCM = w_C \cdot Choice + w_A \cdot Access$

Anticipated Results

Our anticipated results for this work-in-progress research study are four folds. First, the response and completion rate from the Delphi expert panel is expected to be less than 100%, but still high enough (around 70% or more) for a good representation of the group. Second, because the Delphi expert panel methodology will be used, it is expected that the expert panel will have different perspectives, and, therefore, it will take several iterations to reach consensus to develop the final version of the PIPVI benchmarking instrument with the weight distribution for the various components of the PIPVI. Third, it is expected that after data collection, our results are expected to reveal if there are statistical mean differences in PIPVI, DPPPM, OPISM, and OPCCM between 50 Websites of pharmaceutical companies that market birth control versus 50 Websites of pharmaceutical companies that market allergy medications. Last, the results are also expected to reveal if there are any significant differences in the pharmaceutical company's PIPVI, DPPPM, OPISM, and OPCCM based on its headquarters' country, size, and reported annual revenues.

Discussions and Conclusions

Because incidents continue to rise due to companies' misuse of consumer information (Anton et al., 2010; Lanier & Saini, 2008; Pollach, 2007), this work-in-progress research study will attempt to address the proliferation of online privacy violations by companies. We will do so by developing a PIPVI benchmarking instrument, including its essential hierarchical components to assess documented and online practices implemented on Websites. This work-in-progress research study will achieve the seven goals with a three phased approach. First, an expert panel using the Delphi expert methodology will be 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 benchmarking instrument will be used to assess the documented and online practices implemented on 100 pharmaceutical companies' Websites. Last, a comparison report will be developed for 50 Websites of pharmaceutical companies that market birth control versus 50 Websites of pharmaceutical companies that market allergy medications.

As any other research study, we expect this one to have some limitations. One of the main significant limitations of our study will be that 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 progress or the use of the benchmarking index on different companies may yield different values. While the sample size of 100 companies is valid, further studies can use larger sample size to increase validation of the results and generalizability.

Recommendations and Future Research

This work-in-progress research study outline the research plan to develop a set of measures and a single composite index based upon hierarchical criteria identified by current U.S. laws and regulations recommended for ethical business practices for online transactions. The weights of the hierarchical criteria and composite index will be developed using a Delphi approach. Following, we're planning to carry out the actual development of the proposed PIPVI, collect and analyze the data following the research outline plan discussed here. The findings and the results of the statistical analyses will then be 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). 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.

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.

Bhuleskar, R., Sherlekar, A., & Pandit, A. (2009). Hybrid spam email filtering. *First International Conference on Computational Intelligence, Communication Systems and Networks,* India, 302-307.

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.

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. (n.d.). *About the Federal Trade Commission*. Retrieved on March 1, 2012, from http://ftc.gov/ftc/about.shtm.

Federal Trade Commission. (2010). *Unfairness and deception: Enforcement.* Retrieved on October 11, 2012, from http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

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, 2012, 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 U.S. 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. (2010, November 15). *The Internet crime complaint center hits 2 million.* Retrieved October 14, 2010, 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.

Jain, C. L. (1985). Delphi - forecast with experts' opinion. *Journal of Business Forecasting, 4(*4), 22-23.

Jaisingh, J., Barron, J., Mehta, S., & Chaturvedi, A. (2008). Privacy and pricing personal information. *European Journal of Operational Research, 187*, 857-870.

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.

Kelly, E. P., & Rowland, H. C. (2000). Ethical and online privacy issues in electronic commerce. *Business Horizons,* 3-12.

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. (2000). Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing, 19*(2), 238-249.

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.

Nhan, J., Kinkade, P., & Burns, R. (2009). Finding a pot of gold at the end of an Internet rainbow: Further examination of fraudulent email solicitation. *International Journal of Cyber Criminology*, *3*(1), 452-475.

Palmer, E. (2012, September 20). *Bayer takes aim at J & J Evra with new birth control patch*. Retrieved September 22, 2012, 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.

Poddar, A., Mosteller, J., & Ellen, P. S. (2009). Consumers rules of engagement in online information exchanges. *The Journal of Consumer Affairs*, *43*(3), 419-448.

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

Privacy Rights Clearinghouse. (2011). *Chronology of data breaches: Security breaches 2005–present*. Retrieved on December 10, 2012, from http://www.privacyrights.org/data-breach.

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.

Schwaig, K. S., Kane, G. C., & Storey, V. C. (2005). Privacy, fair information practices and the fortune 500: The virtual reality of compliance. *The DATA BASE for Advances in Information Systems*, *36*(1), 49-63.

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.

Storey, V. C., Kane, G. C., & Schwaig, K. S. (2009). The quality of online privacy policies: A resource-dependency perspective. *Journal of Data Base Management*, *20*(2), 19-37.

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.

Xie, E., Teo, H-H., & Wan, W. (2006). Volunteering personal information on the Internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Market Letters*, *17*, 61-74.

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.

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.

Biographies

Shonda D. Brown is a manager at a Fortune 500 global health service and insurance provider company. She is currently pursuing a Ph.D. in Information Systems with a concentration in Information Security at Nova Southeastern University. Her research interests include information security and privacy. She has served 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 a Professor at the Graduate School of Computer and Information Sciences at 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 e-learning systems, cyber-security skills, and cognitive value of information systems. Dr. Levy is the author of 'Assessing the Value of e-Learning Systems' (2006). 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 IS, Information Security, and online learning topics. Dr. Levy's teaching interests in the masters level include MIS, system analysis and design, information systems security, e-commerce, and Web development. His teaching interests in the doctoral level include Information Systems Development (ISD) and Advanced Multivariate Research Methods and Statistics. To find out more about Dr. Levy, please visit his site: http://scis.nova.edu/~levyy/