

2015


# Identifying Unethical Personally Identifiable Information (PII) Privacy Violations Committed by IS/IT Practitioners: A Comparison to Computing Moral Exemplars

Mark H. Rosenbaum

Nova Southeastern University, [mhrose8989@gmail.com](mailto:mhrose8989@gmail.com)

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: [http://nsuworks.nova.edu/gscis\\_etd](http://nsuworks.nova.edu/gscis_etd)

 Part of the [Computer Sciences Commons](#), and the [Social and Behavioral Sciences Commons](#)

## Share Feedback About This Item

---

### NSUWorks Citation

Mark H. Rosenbaum. 2015. *Identifying Unethical Personally Identifiable Information (PII) Privacy Violations Committed by IS/IT Practitioners: A Comparison to Computing Moral Exemplars*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (29) [http://nsuworks.nova.edu/gscis\\_etd/29](http://nsuworks.nova.edu/gscis_etd/29).

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact [nsuworks@nova.edu](mailto:nsuworks@nova.edu).

Identifying Unethical Personally Identifiable Information (PII)  
Privacy Violations Committed by IS/IT Practitioners: A Comparison to  
Computing Moral Exemplars

by

Mark H. Rosenbaum

A dissertation submitted in partial fulfillment of the requirements  
for the Degree of Doctor of Philosophy  
in  
Information Systems

Graduate School of Computer and Information Sciences  
Nova Southeastern University

2015

An Abstract of a Dissertation Submitted to Nova Southeastern University  
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Identifying Unethical Personally Identifiable Information (PII)  
Privacy Violations Committed by IS/IT Practitioners: A Comparison to  
Computing Moral Exemplars

by  
Mark H. Rosenbaum

2015

In some instances, Information Systems and Information Technology (IS/IT) practitioners have been noted to commit privacy violations to Personally Identifiable Information (PII). However, computing exemplars, due to their notable dispositional Hallmark Features of morality, understandings of ethical abstractions, and other components that comprise their virtuous makeups, are theoretically less likely to commit privacy violations to PII. This research attempted to verify if those IS/IT practitioners who identify with some of the Hallmark Features of moral and computing exemplar were less willing to commit privacy violations to PII than were those IS/IT practitioners that did not identify themselves with some of the Hallmark Features of moral and computing exemplars. In order to accomplish this, this research developed and validated two new survey instruments capable of identifying those IS/IT practitioners that were more and less willing to commit unethical privacy violations to PII, and contrast them against some of the Hallmark Features of computing exemplars. The findings of this research supported the conclusion that IS/IT practitioners that identify with some of the Hallmark Features of moral and computing exemplars were less willing to commit privacy violations to PII than were other IS/IT practitioners. Specifically, the results indicated that the most prominent predictor to indicate a lesser willingness to commit privacy violations to PII was that of those IS/IT practitioners that displayed prosocial orientations. Additionally, the predictors of age, level of education, and how ethical IS/IT practitioners assessed themselves to be, proved to be significant markers for those individuals that were less willing to commit privacy violations to PII. While the results are promising, they are also alarming, because the results also indicate that IS/IT practitioners are blatantly willing to commit privacy violations to PII. Thus, two immediate implications resonate from the results of this research. First, there are those individuals that have been given the trusted position of guardianship for society's personal information that should probably not have it, and secondly, further investigations are warranted to determine what other predictors may promote a lesser willingness to commit privacy violations to PII. The contribution of this research to the fields of IS/IT, personnel selection and testing, and organizational assessment and training is unique. This is because, to date, no other discernable literatures have ever investigated the rating and rankings of the severity of PII privacy violations, nor has any other research investigated what Hallmark Features of individuality contribute to a less willing disposition to commit PII privacy violations.

## Acknowledgements

Though he has passed many years ago, I dedicate this dissertation to my grandfather, a man whom I sorely miss and often think of with great fondness.

All journeys begin with the first step, as did this dissertation. It represents the culmination of much work, none of which would have been possible if it were not for the encouraging support of others. I would like first to thank my parents for supporting my educational dreams.

The process of writing a dissertation is often the largest roadblock for aspiring scholars, unless you have dissertation committee members that are your friends, mentors and allies. To my dissertation committee members I say, "If I can give back to other students in the ways that you have given to me, then one day I may too be an educator to admire, as I so admire all of you." Additionally – To my chair and friend Dr. Ling Wang, I would like to say the following. How fortunate I have been to have such a wonderful and caring person guide me through the most important thing I have ever written. As chairs go, you were always consistent, very positive, and always made time for me. How could a student ever ask for more? I knew I liked you the first day that I walked into your statistics and methodologies course. Thank you for all that you are and all that you have done for me, I am forever in your debt. To my committee member Dr. Chuck Huff, your magnificent research with computing exemplars, lets everyone in the field of IS/IT know that there are still those individuals in the world that have care and respect for others. Thank you for his unwavering belief in my abilities, and guidance when direction was lost. In appreciation of all the literature that you shared with me, the more than 200 emails that went back and forth between us, and the enumerable hours of conversation over the telephone, I am forever grateful. Lastly, I thank you for being a friend in the darkest of hours of my life when I was dealing health issues. To my other committee member Dr. Glyn Gowing who allowed me early on to start developing the ideas for this dissertation in his classes, I want you to know that without your encouragement and guidance this research may have never taken place. Lastly, here is a warm felt sense of appreciation for Dr. William Hafner for helping me begin this journey, and Dr. Marti Snyder for just being you.

With my deepest regards, much love and appreciation to all – Thank you for all that you gave of yourselves.

## Table of Contents

Abstract	ii
Acknowledgements	iii
List of Tables	viii
List of Figures	ix

### Chapters

#### **1. Introduction 1**

Background	1
Introduction to PRIMES	2
Understanding IS/IT Practitioners and Privacy Impacts	4
Ethical Conceptualizations	5
Understanding IS/IT Privacy Violations to PII	10
Problem Statement	16
Dissertation Goal	16
Hypothesis	17
Relevance and Significance	18
Barriers and Issues	22
Limitations	23
Delimitations	25
Definition of Terms	26
Summary	29

#### **2. Review of the Literature 31**

Introduction	31
Moral Philosophy	35
Virtue Ethics	36
Moral Exemplars	39
Exemplar Moral Development	40
Exemplar Influences	42
Personality	43

## **2. Review of the Literature (cont.)**

Integration of Morality into a Self-system 44

Moral Ecologies 45

Organizational Structures 46

Codes of Ethics and Training 47

Moral Skills and Knowledge 50

Mentoring 52

Intermediate Concepts and Role Specific Obligations 53

Other Exemplar Factors 55

Hallmark Features 55

Professional Identity 61

Computing Exemplars 63

Summary 69

## **3. Research Methodology 71**

Introduction 71

Methods 72

Phase One Development 72

SME Population 73

Data Collection 75

Data Analysis 76

Descriptive Statistics 76

Reliability 76

Validity 77

Phase Two Development 77

Population Sample 81

Data Collection 82

PPVS Data Analysis 83

Descriptive Statistics 83

Inferential Statistics 84

Summary 84

#### **4. Results 87**

Overview 87

Subject Matter Experts Pre-Privacy Violations Survey 87

IS/IT Practitioners PII Privacy Violations Survey (PPVS) 88

Pre-Analysis Data Screening and Cleaning 89

PII Privacy Violations Scale-1 (PPVS-1) 92

PII Privacy Violations Scale-2 (PPVS-2) 98

PII Privacy Violations Scale-3 (PPVS-3) 104

Summary 109

#### **5. Conclusions, Implications, Recommendations, and Summary 113**

Introduction 113

Conclusions 113

Implications 128

Recommendations 130

Summary 132

#### **Appendices 136**

Appendix A – Aristotle’s 12 Virtues, Vices, and Deficiencies 137

Appendix B – Neo-Aristotelian Virtues 138

Appendix C – Murphy’s International Marketing Virtues 139

Appendix D – Blasi’s Ordered Virtue Skills 140

Appendix E – Ethical Skills Required for Ethical Ability 141

Appendix F – Four Processes, Their Skills, and Sub-skills 142

Appendix G – Attributes of Professionalism in Computing 145

Appendix H – Four-Component Model of Moral Action in Computing 146

Appendix I – SMEs PPSS 148

Appendix J – SMEs Invitation to Participate Email 171

Appendix K – Introduction to PPSS Survey for SMEs 172

Appendix L – Introduction and Instruction Letter to SMEs for PPSS Survey 173

Appendix M – SMEs Demographics 175

Appendix N – SMEs PPSS Measures of Central Tendency 178

Appendix O – Privacy Violation Questions Descending Mean Values	180
Appendix P – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted	211
Appendix Q – SMEs Privacy Violation Questions Response Frequencies	213
Appendix R – PPVS Hallmark Features Section	233
Appendix S – PPVS-1 15 Privacy Violations to PII	252
Appendix T – PPVS-2 15 Privacy Violations to PII	261
Appendix U – PPVS-3 15 Privacy Violations to PII	270
Appendix V – Survey Participation Email Invitation Letter	280
Appendix W – Survey Invite Email Distributed by CIOs, CISOs, and CPOs	281
Appendix X – Technology-base Job Titles	282
Appendix Y – LinkedIn Country Search	284
Appendix Z – LinkedIn Company Search	285
Appendix AA – SurveyGizmo Participation Introduction	288
Appendix AB – PPVS-1 Demographics	289
Appendix AC – PPVS-1 Correlations Table	302
Appendix AD – PPVS-2 Demographics	305
Appendix AE – PPVS-2 Correlations Table	311
Appendix AF – PPVS-3 Demographics	314
Appendix AG – PPVS-3 Correlations Table	324

<b>References</b>	327
-------------------	-----



## **List of Tables**

### **Tables**

1. Cyber-Ark Comparison of 2009/2008 Security Survey Data 13
2. PPVS-1 Descriptive Statistics for Regression Model 97
3. PPVS-1 Regression Coefficients and VIFs for Privacy Violations to PII 98
4. PPVS-2 Descriptive Statistics for Regression Model 102
5. PPVS-2 Regression Coefficients and VIFs for Privacy Violations to PII 103
6. Time Tables to Complete the Three PPVSs 105
7. PPVS-3 Descriptive Statistics for Regression Model 108
8. PPVS-3 Regression Coefficients and VIFs for Privacy Violations to PII 109
9. Components of Personality Markers to Measure 131

## List of Figures

### Figures

1. PRIMES 3
2. Hierarchical Ethical Conceptualizations 3
3. Process of Knowledge and Understanding to RSOs 7
4. ICs Hierarchy for Respecting Privacy as Applied to Data Mining and PII 7
5. Residual Plot for PPVS-1 92
6. Residual Plot for PPVS-2 93
7. Residual Plot for PPVS-3 93

# Chapter 1

## Introduction

### Background

Today's interconnected Information Systems and Information Technology (IS/IT) climates have provided some of humanity's greatest opportunities and achievements, as well as allowed greater access to information. Due to this increased access to information, society must now, more than any other time in its history deal with the misuse and abuse of these systems by unethical individuals, this is particularly true for members of society who have found that their digital Personally Identifiable Information (PII) has been compromised by those entrusted to protect it.

A problem in the technology field is that some IS/IT practitioners have committed privacy violations to PII, and have accessed confidential or sensitive information with their administrative password (Cyber-Ark, 2009, 2011; Kuo, Lin, & Hsu, 2007). Arguably, this is not only a privacy violation committed towards the information, but also against the person whose information it is. Additionally, these violations may also carry the distinction of being both immoral and illegal (Post, 2001; Quallen, 2009; Romanosky & Acquisti, 2009). For the purpose of this dissertation, PII privacy violations are unauthorized information intrusions obtained from digital data that have the potential for causing economic harm or psychological pain. These data intrusions may include, but are not limited to, violations committed against passwords, digital identification cards, banking information, medical records, e-mails, names, addresses, social security numbers, etc. For example, obtaining personal medical records of an individual without authorization is a privacy violation to PII.

Society has voiced concerns regarding PII for over 120 years (Warren & Brandies, 1890). By the mid-70s, PII and its confidentiality became a heightened concern due to digitized information stored in databases (Bynum, 2001). Ghosh and Turrini (2010) now believe that digitized PII is under continual threat of exposure and disclosure. This is because of individuals' willingness to commit privacy violations to PII. Criminals and hackers are not the only individuals that pose threats to PII (Bishop, 2006; Smith, 2009). For example, Cyber-Ark (2010), and Kuo et al. (2007) have noted that some IS/IT practitioners pose threats to PII, because they too are willing to commit privacy violations to PII.

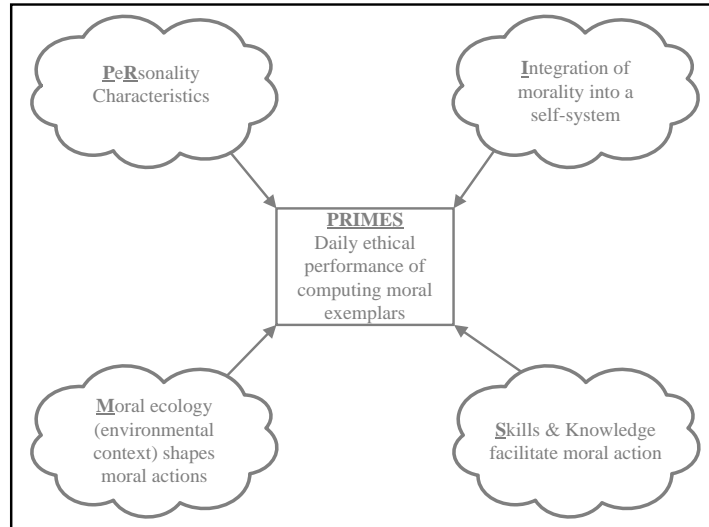
**Introduction to PRIMES.** However, Huff, Barnard, and Frey (2008a, 2008b) indicate an altogether differing, and positive view of some IS/IT practitioners. Based upon their four component *theoretical model* of PRIMES, they suggest that computing exemplars may be less inclined to commit privacy violations to PII. Simply, computing exemplars represent the highest standards of moral integrity, and display exemplary ethical actions within their profession. Huff et al. (2008a) define PRIMES in the following manner.

The model we present here grounds moral action in relatively stable Personality characteristics, guides moral action based on the Integration of Morality into the self-system, shapes moral action by the context of the surrounding Moral Ecology, and facilitates moral action with morally relevant Skills and knowledge (thus the PRIMES acronym). The model seeks to explain the daily performance of moral action of computing professionals and to illuminate ways that computing professionals might be trained to be more active, ethically committed, and

ethically effective in their daily performance, across the lifespan of their careers.

(p. 285)

Graphically one can think of PRIMES in the following manner (Figure 1.)



*Figure 1. PRIMES*

Based on virtue ethics, PRIMES integrates aspects of personality theory, moral development theory, environmental ecologies, and expert skills and knowledge to explain the moral behaviors and ethical actions of computing exemplars. Additionally, PRIMES accounts for the lifelong learned domain-specific skill-sets known as Intermediate Concepts (ICs) and Roles Specific Obligations (RSOs). It is in part due to ICs and RSOs that computing exemplars have the know-how and ability to act ethically in their profession; this may account for why these exemplars are possibly less likely to commit privacy violations to PII. As defined by Bebeau and Thoma (1999), ICs represent core ethical conceptualizations necessary for decision-making within a practitioner's career domain. Therefore, ICs act as a means of professional guidance. According to Keefer and Ashley (2001), RSOs relate to ICs as the conduit of action. RSOs represent action

specific behaviors of ICs. Therefore, RSOs would indicate knowledge and understanding for the ethical conceptualizations within one's career domain.

**Understanding IS/IT practitioners and privacy impacts.** Identifying and understanding the personal dispositions of IS/IT practitioners that are likely to commit privacy violations to PII is necessary in order to protect the security of PII. It is also necessary to understand which IS/IT practitioners are more likely to commit privacy violations to PII because of the societal expectations that individuals have for their personal information (Nissenbaum, 2010). Singularly, privacy violations to PII can, and do cause pain and suffering (Newman & McNally, 2005; Solove, 2006). Both, the pain and suffering associated with PII privacy violations tie to economic loss and psychological anguish (Holtzman, 2006; Moor, 1990). Furthermore, society's increased reliance on technology has made PII more susceptible to intrusive violations. Because of the widespread use of technology, and the greater number of personal privacy violations carried out with technology, technology's impact upon privacy needs closer scrutinization (Stahl, 2004; Waldo, Lin, & Millett, 2010).

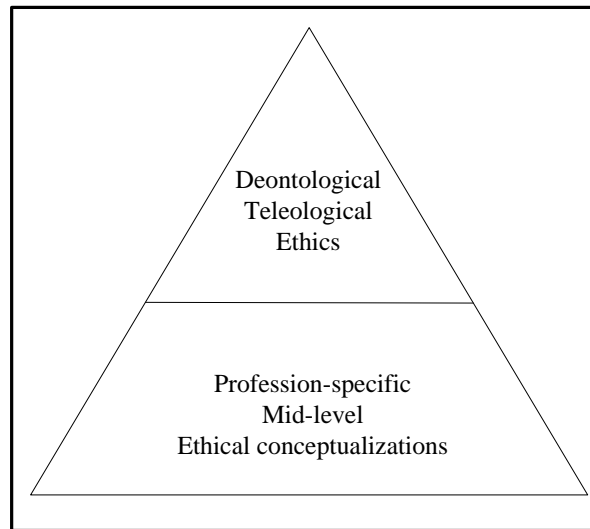
According to Kuo et al. (2007), IS/IT practitioners represent one group of individuals that society has charged with the stewardship for protecting data privacy, and particularly PII. Freund (2006) suggested that IS/IT practitioners are "privacy guardians" (p. 419). Previously, Oz (1993) pointed out that it is the impact of these practitioners' behaviors, and how they manage information systems that raise issues in privacy. Chow (2001) suggested that ethically responsible behavior for IS/IT practitioners involves moral decision-making. Kuo et al. also echoed this sentiment, particularly for PII. Hence, protecting PII is more than just a technical or policy issue, it is dependent upon

moral human behaviors (Power, 2007). However, moral and professionally responsible computing behaviors require professional virtue skills and knowledge as a prerequisite to virtuous computing behavior (Huff et al., 2008a, 2008b; O'Boyle, 2002). For the IS/IT practitioner this would mean a knowledge and understanding for matters such as privacy law, encryption, social engineering, code of ethics, and other similar facets germane to the professional practice of computing. Additionally, ethical decision-making in the field of IS/IT privacy requires an ability to understand the conceptualizations of fine-grained ethical abstractions that are related to computing.

**Ethical conceptualizations.** Modern theory assessing an individual's ethical conceptualizations about abstract moral reasoning, judgment, and decision-making originated with Kohlberg (1969, 1984), and Rest (1975, 1979). Kohlberg's and Rest's contributions to moral development theory and decision-making laid the groundwork for understanding how individuals formally develop a sense of what is morally right from wrong. One of the most profound differences between Kohlberg's and Rest's model is how developmental stages progress within an individual. Kohlberg believed that individuals progressed from one developmental stage to the next; therefore, an individual could only move to the next stage in moral development after they had completed the previous stage. However, Rest thought that moral development was dynamic, and that individuals could fluidly move back and forth between stages. This could explain why in some circumstances an IS/IT practitioner would choose or not choose to protect PII privacy. One important insight gained from both Kohlberg and Rest is that, if ethical development were not possible, ethical instruction would be irrelevant, and therefore, assessment of moral reasoning and development would not be necessary (Woodward,

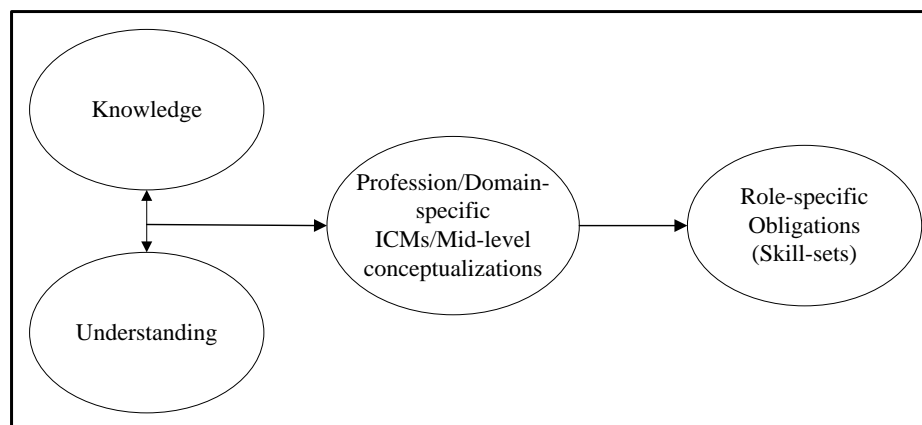
2007). Both moral development models focused on course-grained high-level ethical abstractions like justice and fairness (Walker, 2002a; Woodward). In this sense, both models referred to the deontological and utilitarian conceptualizations that a society or culture bases their norms and values upon (Ishida, 2006). Therefore, these high-level abstractions are society's foundational and guiding behavioral standards or principles. However, morally responsible behaviors for practitioners within career domains such as medicine, engineering, and IS/IT require specialized fine-grained ethical knowledge and understandings that are domain specific (Bebeau & Thoma, 1999; Huff et al., 2008a, 2008b; Keefer, 2005; Pritchard, 1998). This knowledge and understanding allow practitioners to act in accordance to their Role Specific Obligations (RSOs). According to Keefer and Ashley (2001), RSOs represent the professional knowledge, understandings, and training that aid practitioners' in their moral decision-making, and that guide their normative behaviors. For Keefer and Ashley, knowledge and understanding represent mid-level principles or principles of morality once removed from the highest level of abstraction, such as those principles of morality described in deontological and utilitarian ethics. That is to say; these mid-level conceptualizations are likely to sit hierarchically one level lower than the deontological or utilitarian ethical abstractions that Kohlberg and Rest spoke of (Figure 2).





*Figure 2. Hierarchical Ethical Conceptualizations*

As such, these profession-specific mid-level ethical principles come from provisions within the codes of ethics for a given field of practice (Bebeau & Thoma, 1998, 1999; Keefer & Ashley). Just as Keefer and Ashley, used the term mid-level principles, Bebeau and Thoma (1998, 1999) used the term Intermediate Concept (ICs). Both ICs and mid-level principles are the profession-specific, or domain-specific ethical conceptualizations acquired through knowledge and understandings. They allow practitioners the ability to act with moral integrity within their profession (Figure 3).



*Figure 3. Process of knowledge and understanding to RSO's*

Frequently mentioned in the field of computing, privacy is a concept that requires ethical consideration and conceptualization (Mason, 1986; Moor, 1997, Nissenbaum, 2010; Stahl, 2004). Peslak (2007) supports this conclusion with data indicating that privacy is considered an important ethical issue when viewed in terms of information technology. Additionally, Peslak (2006) notes that the *respect* to PII privacy has become a factor of importance when discussing IS/IT privacy related matters. From this, one might surmise that privacy and respect represent ICs. Further support for this supposition came from Bebeau and Monson (2008) when they noted that ICs often come from professional codes of ethics. In this instance, an inspection of both the ACM and IEEE codes of ethics indicate that respect and privacy are mentioned as aspects of professional consideration in the field of computing. This provides a clear indication that privacy is an important ethical issue when viewed in terms of information technology. Therefore, it is no irony that Huff and Frey (2005) specifically cite privacy as an IC in the field of technology. Additionally, by its implied and inherent association to privacy, informed consent (Huff & Frey; Tavani & Moor, 2001), data mining (Fule & Roddick, 2004; Nissenbaum, 2010; van Wel & Royakkers, 2004), and PII (Kuo et al., 2007) represent profession-specific ICs in IS/IT. In the case of privacy and informed consent, it is the practitioner's knowledge and understandings of end-users opting-in and opting-out of PII policies that guide their RSOs for respecting and protecting PII privacy. Additionally, this respect and understanding of opting-in and opting-out of PII privacy, informs the IS/IT practitioner how PII is to be accessed, and under what conditions the information can be used. In part, it is this type of specialized knowledge and understanding for the ethical principles of opting-in and opting-out that allow IS/IT practitioners to act morally with regard to their RSOs towards respecting the privacy to PII.

As noted previously, association codes of ethics contain ICs. For instance, the ACM both conceptualizes and address the concepts of privacy, respect, PII, and informed consent in sections 1.1, 1.4, 1.7, 1.8, 2.3, and 3.5 of their codes of ethics (ACM Code of Ethics, 1992). Because PII represents distinguishingly identifiable characteristics of a particular person (Krishnamurthy & Wills, 2010), its non-acquisition and non-distribution is critical as an aid in the prevention of identity related theft or fraud from those not authorized to have access to this type of information. In terms of the IC of respect, *privacy* hierarchically sits below the profession-specific principle of respect, which requires knowledge and understanding within the professional working schema of the IS/IT practitioner, and represents a domain-specific concept (Figure 4). As a domain-specific concept, privacy also relates to the (sub)-domain-specific concept of *data mining* and the other related ICs to data mining such as PII, non-acquisition and non-distribution of PII, and ID theft and ID fraud (Figure 4).

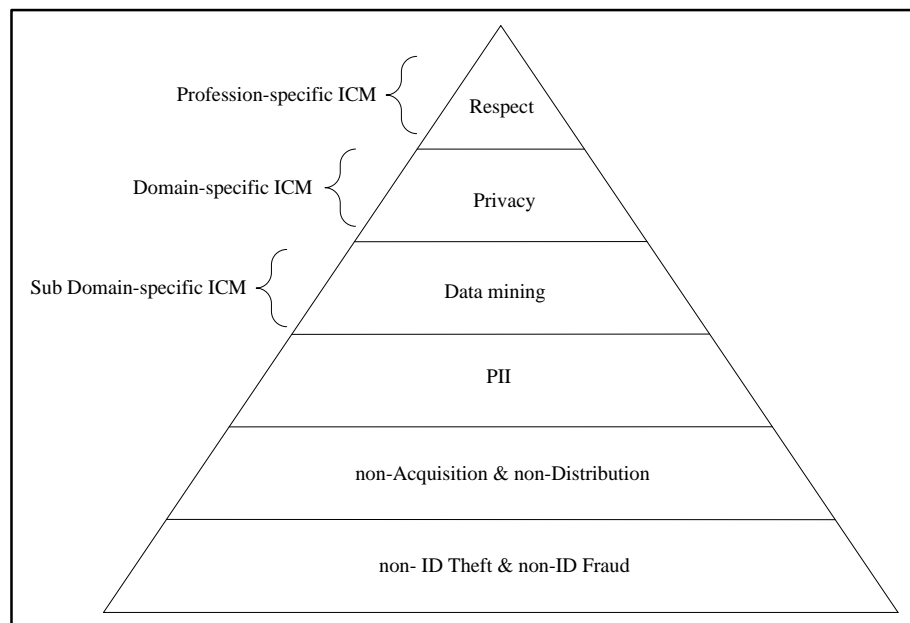


Figure 4. ICs hierarchy for respecting privacy as applied to data mining and PII

Through the morally appropriate RSOs of non-acquisition and non-distribution to PII in data mining, the IS/IT practitioner is exhibiting his or her knowledge and understanding for the professional conceptualizations of respect, privacy, informed consent, PII, and data mining. It is in the form of these professional understandings and knowledge that the ICs of non-acquisition and non-distribution to PII should in theory, and application, act as preventative moral measures that safeguard identity theft, or identity fraud.

However, not all IS/IT practitioners' behavior towards the privacy to PII is ethical (Chung & Khan, 2008; Cyber-Ark, 2008a, 2008b, 2009, 2010).

**Understanding IS/IT privacy violations to PII.** According to Brooks (2008), IS/IT technology practitioners have privileged access to personally private and corporate information, they also have the expertise to manipulate information. By means of this power, practitioners' carry a responsibility for protecting society's digitally private information. Brooks's references to the magnitude of moral responsibility, the power that IS/IT practitioners have for protecting private information, and their RSOs, imply the necessity of a high moral quality for the behavioral practices towards privacy. Stahl (2004) maintains that decisions about privacy are affected by how individuals shoulder the obligations for how privacy should be handled. Therefore, decisions regarding privacy acquire a moral decision-making component. Stahl also maintains that the relationship between privacy and moral responsibility is complex, yet worthy of ethical consideration. Additionally, Stahl also maintains that part of this consideration is the important relationship that the subject, that is to say the IS/IT practitioner, has with the object, in this case privacy.

While IS/IT practitioners have the assigned jurisdiction of digital privacy protection (Kuo et al., 2007), little work has been done to assess their moral reasoning, decision-making attitudes, and behaviors towards privacy. What research that does exist, aside from the Huff et al. (2008a, 2008b) action-oriented model of PRIMES, originated with the Banerjee, Cronan, and Jones (1998), and the Bommer, Gratto, Gravander, and Tuttle (1987) behavioral models of ethical and unethical decision-making in IS/IT. Based on the works of Banerjee et al. and Bommer et al., other models have been developed that explain ethical decision-making from various focal points that include, but are not limited to, the context of situational influences, individual characteristics, moral intensity, and environmental contexts. More recently, Cronan and Douglas (2006, 2008) proposed an Information Technology (IT) ethics-based model that suggests ethically based behavioral intention is influenced, and possibly determined by attitude, which in turn is influenced by myriad other factors. When comparing models, a central point of divergence is that the PRIMES model is action-oriented, and the other models are decision-oriented. In this sense, an action-oriented model not only explains particular behaviors, but it does so in terms of behaviors that can be observed.

To date only Kuo et al. (2007) have produced literature demonstrating action-based choices in an empirical investigation of IS/IT practitioners' moral reasoning, decision-making attitudes, and actions towards PII privacy protection. However, the Kuo et al. research only provides a glimpse of privacy behavior based on reported self-efficacy. In part, it may be due to this lack of a privacy-based metric that measures action choices that Huff et al. (2008b) mentions the need for such an instrument. The need for this type of assessment is further justified on four fronts. First, many of the IS/IT students of today will be the IS/IT practitioners of tomorrow, and they have demonstrated

questionable understandings for what moral and immoral behaviors are in the IS/IT field (Peslak, 2007; Namlu & Odabasi, 2007; Woodward, Davis & Hodis, 2007). Second, much privacy-based research has used student populations, which caused Belanger and Crossler (2011) to state:

The review of the literature reveals that information privacy is a multilevel concept, but rarely studied as such. We also find that information privacy research has been heavily reliant on student-based and USA-centric samples, which results in findings of limited generalizability... We call for research on information privacy to use a broader diversity of sampling populations, and for more design and action information privacy research to be published in journal articles that can result in IT artifacts for protection or control of information privacy (p. 1017).

Third, Kuzu (2009), revealed that “ICT professionals” (p. 91) were not sure how to define computer ethics, and often did so in terms of citing immoral computing behaviors. One can state the importance of Kuzu’s finding in the following manner: *knowing what is wrong or unethical, is not necessarily proceed by knowing what is ethically right*. Lastly, IS/IT practitioners are noted for displaying unethical work related behaviors. For example, Chung and Khan (2008) identified 43 unethical behaviors that could be committed by IS/IT practitioners, and demonstrated that all unethical acts were not equal in severity. While Chung and Khan provide a picture for some of the types and categories of unethical IS/IT behaviors, they miss many PII privacy violation types and categories. Similarly, surveys conducted by Cyber-Ark (2008a, 2008b, 2009, 2010) revealed that IS/IT practitioners have been committing immoral behaviors and that they do so by using the tools of their trade. For instance, Cyber-Ark (2008a) surveyed 300 IT

administrators and found that 88% of these employees would steal company secrets if they had knowledge of a layoff. The target information in a number of instances included CEOs passwords, database information, financial information, and R&D plans. Additionally, 47% of respondents reported to having accessed information not relevant to their jobs, and 33% stated that they had used their administrative password to retrieve confidential information. Conducted in New York, London, and Holland, the Cyber-Ark (2008b) survey data indicated that some IT workers stated that if they were fired tomorrow, they would take legal records, passwords, HR records, plans and proposals, and customer contact database information. Exact percentages of who would take what varied by country of origin, yet the majority respondents stated that they would either carry the information out by thumb drive or e-mail it to themselves. The data collected from more than 400 IT administrators by Cyber-Ark (2009), indicated even more troubling matters for privacy when compared to the previous year's data. Table 1 represents what aspects of information that IT administrators would steal if fired.

**Table 1.** Cyber-Ark comparison of 2009/2008 Security Survey Data

<b>Type of Information</b>	<b>2009</b>	<b>2008</b>
Customer Database	47%	35%
Email Server Admin Acct.	47%	13%
M&A Plans	47%	7%
R&D Plans	46%	13%
CEO's Password	46%	11%
Financial Reports	46%	11%
Privileged Password List	42%	31%

A comparison between the 2008 data and the 2009 data indicates an increase in every category of measurement. These increases in privacy violations do indicate higher levels of unethical, illegal, and dishonest behaviors. Also standing out in Table 1 is the markedly sharp increase in the theft of information that provides companies with competitive advantages. Merger and Acquisition (M&A) plan theft increased 40%, R&D plan theft escalated by 33%, and theft of Financial Reports expanded to 45%. An indicator not present on Table 1 is a 33% increase between 2008 and 2009 with those IT employees that stated they have accessed corporate information without authorization. From an information security standpoint, one has to question whether or not security measures had been circumvented, or if IT workers simply used their passwords to access information.

On the surface, the Cyber-Ark surveys may look suspicious, even bias considering that the company's mission is to sell security protection software. However, a survey sponsored by the Symantec Corporation, and conducted by the Ponemon Institute (Messmer, 2009), identified that out of the 945 workers polled, 20% or 188 workers identified themselves as corporate information technologists who would steal or had stolen confidential corporate information. Seventy-nine percent of the 945 workers admitted that stealing is wrong, but concluded, "Everyone else does." Given the Cyber-Ark and Symantec data, one could conclude that the IS/IT industry faces some difficult issues concerning unethical decision-making and immoral actions that are sometimes taken towards PII privacy.

Recognizing that deficits in moral reasoning, judgment, and decision-making exist within the IS/IT field, Woodward (2007), Woodward and Ashby (2006), and Woodward, Davis, and Hodis (2007) have called for an IC instrument to assess IS/IT



moral reasoning and decision-making for professional domain-specific ethical principles based on the work of Bebeau and Thoma (1998, 1999). Specifically, Huff et al. (2008b) suggested an assessment instrument that would measure moral reasoning and decision-making for privacy.

Previously presented literature points to how IS/IT practitioners are not displaying good computing behaviors. However, Huff et al. (2008a, 2008b) draws attention to what good computing is in the personification of computing moral exemplars with the PRIMES model. PRIMES represents a schematic model that describes computing exemplar's behaviors. The model is based on the stable personality characteristics of a moral self-system that integrates professional skills, knowledge, and understandings of ICs into RSOs. In addition, the model facilitates moral action in the field of IS/IT. Organized around components of virtue ethics, moral philosophy, psychology, skills and knowledge, and moral ecologies, PRIMES represents a theoretically integrated and applied model describing the forces that act internally and externally on computing exemplars. Therefore, one could argue that PRIMES is an actual depiction of the forces that shape and guide the moral actions of computing exemplars. For this reason, PRIMES is also a model of action and a model in-action that explains the moral behaviors and decision-making influences for computing exemplars.

Because PRIMES was developed to explain the sustained moral actions of computing practitioners', with an aim on developing a pedagogical approach for teaching computer ethics, one of the suggestions that Huff et al. (2008b) makes, is to develop an IC profession-specific instrument that assess IS/IT practitioners' moral reasonings, judgments, and decision-making. Specifically, this recommendation is for a profession-specific instrument that focuses on the moral assessment and decision-making of

practitioners' privacy understandings. This type of instrument would give an indication for how practitioners might behave towards IS/IT privacy related issues. Further justification for such an instrument is that, moral behavior requires recognizing the opportunity to take moral action (Huff et al.; Bebeau & Thoma, 1998, 1999), but recognition is only half the process; one must be willing to implement the morally correct action. Thus, if one were to act in a morally self-regulatory manner that is consistent with one's RSOs, it would be an indication of knowledge and understanding for privacy ICs. Therefore by understanding virtue ethics, and the PRIMES model of virtuous computing, researchers would be able to identify non-virtuous and immoral IS/IT PII privacy related behaviors, and those IS/IT practitioners that are likely to commit violations to PII privacy. This can be accomplished by contrasting computing exemplars Hallmark Features and professional domain-specific knowledge of PII privacy violations that are based on ICs, against IS/IT practitioners that do not possess these qualities.

### **Problem Statement**

A problem in the ICT field is that some IS/IT practitioners are willing to commit privacy violations to PII (Cronan & Douglas 2006; Cyber-Ark, 2009; Kuo et al., 2007) while others may not be as likely to commit these types of violations (Huff et al., 2008a, 2008b). Presently, no survey instrument is available to assess which IS/IT practitioners are more or less willing to commit these types of violations.

### **Dissertation Goal**

According to Kuo and Hsu (2001), there is a need to study the link between ethical intentions and privacy. Huff et al. (2008b) suggested developing a measurement

instrument to assess IS/IT practitioners' ethical intentions towards privacy that includes adapting ICs from the work of Bebeau and Thoma (1998, 1999). Therefore, the goal of this dissertation was to develop and validate a new survey instrument that would accurately measure if non-exemplar IS/IT practitioners were willing to commit privacy violations to PII, and determine what practitioners would not. Furthermore, this survey instrument will compare and contrast IS/IT practitioners' knowledge and behaviors for PII privacy ICs and RSOs, against the *theoretical* understandings of computing moral exemplars knowledge, behaviors, life styles, and dispositional profiles as defined by Huff et al. (2008a, 2008b), and others. In order to attain this goal, an exploratory, and integrative theoretical analysis based on generalized and somewhat recurring exemplar schemas was employed. Ancillary to this first goal was to demonstrate that those IS/IT practitioners that identified themselves as non-moral computing exemplars were also not acting in accordance to PII privacy ICs and RSOs. To accomplish both goals, a new profession-specific IS/IT, domain-based PII privacy instrument was developed and validated. This privacy violations instrument stands as a measure against which to analyze and contrast exemplar and non-exemplar Hallmark Features, and other elements that may lead to committing and not committing such violations. Because demographic and life experience also influence decision-making behaviors, the survey also attempted to tap factors in these realms that might influence privacy based decision toward PII.

## **Hypothesis**

Based on the PRIMES model (Huff et al., 2008a, 2008b), IS/IT practitioners who do not possess component characteristics of virtuous computing exemplars should be statistically more likely to commit privacy violations to PII than computing moral

exemplars. Postulated on the theorized dichotomy between exemplar and non-exemplar IS/IT computing practitioners, the following hypothesis was generated. IS/IT practitioners who identify themselves as possessing some of the predictive measures of the Hallmark Features that moral and computing exemplars have, will be less likely to commit privacy violations to PII, than those IS/IT that do not identify as possessing some of the Hallmark Features of moral and computing exemplars.

### **Relevance and Significance**

Saia (as cited in Smith, 2002) stated that, “Ethical issues rarely pop up on meeting agendas and in hallway conversations, but they’re always present in information systems” (p. 64). Mujtaba, Cavico, and Sungkhawan (2011) argue that members of society are concerned for the “illegal and unethical decisions of workers and managers” Haines and Leonard (2007a) have stated that “Ethical issues are prominent in the information technology (IT) field” (p. 5). As early as the 1940s and 1950s ethical issues relating to computers, technology, and society were being discussed (Himma & Tavani, 2008). However, it was Parker (1968) that first noted the unethical and illegal behaviors of IS/IT practitioners, and the invasions to privacy that they committed. Davison et al. (2009) suggested that IS/IT practitioner’s moral reasoning towards ethical integrity and accountability is particularly important because of the growing reliance that society has on technology, and therefore it is necessary to study IS/IT practitioners’ ethical behaviors. Peslak (2007) has argued that the ethical issues related to information systems could be a threat to society and its economy. Both Cronan and Douglas (2006), and Leonard and Cronan (2005) have concluded that there is a need to understand the ethical and unethical usage of technology within the IS/IT community because of technologies interrelations

with society, and that unethical behaviors can cause significant losses to business and society, and therefore cause suffering. For example, one prominent interrelation between technology and society is that PII is frequently stored in government and corporate databases. In this regard, unauthorized PII data mining could lead to the access and dissemination of sensitive information such as a driver's license DMV report or, health insurance information that might be used as a prescreening tool for employment. Because of the dependencies that society has on technology, morally appropriate decision-making for how technology is used is necessary. Similarly, an argument can be made for a need to understand the unethical behaviors of IS/IT practitioners because they are the very group of individuals that society has charged with the responsibility for protecting data (Shaw, Ruby, & Post, 1998), and particularly data privacy (Freund, 2006; Kuo et al. 2007).

Limited literature is presently available about PII privacy and the decision-making practices of IS/IT practitioners, therefore, a clear descriptive picture of ethical and unethical PII privacy decision-making behaviors is not possible. For instance, Chung and Khan (2008) identified some 43 unethical IS/IT practitioner behaviors, and concluded that not all behaviors are equal in severity. They based their findings upon the fact that severity of actions can be rated by the potential for loss or gain, the number of individuals involved or affected, societal perception, etc., but of the 43 behaviors, only a few were related to matters of PII. Kuo et al. (2007) also determined that male IS/IT practitioners have a lower self-efficacy for protecting information privacy than do female IS/IT practitioners, and that females have a higher self-efficacy for the non-acquisition of PII. However, Kuo et al. did not investigate the ethical severity of the violations or the myriad types of PII violations that are capable of being committed. Also evidenced in four

separate surveys, Cyber-Ark (2008a, 2008b, 2009, 2010), identified that IS/IT practitioners are committing privacy violations, and in a number of instances these violations were being committed against PII. Furthermore, Prior, Rogerson, and Fairweather (2002) demonstrated that 33% of the members from the Institute for the Management of Information Systems, responded to a survey stating that they found it acceptable to access unauthorized data by using the access code(s) of another individual if that person said they could. An item of importance in the Prior et al. study was that the individuals accessing the data knew they had no authorization to do so, even though the other individual said that they could use their access code. It is critical to note that this type of behavior represents not only a privacy violation, but also identity fraud because one individual is passing himself or herself off as another. Literature from Prior et al., Huff et al. (2008b), and Woodward et al. (2007), indicates that a moral reasoning and decision-making instrument is needed that specifically assesses the career related values and behaviors of IS/IT practitioners. One could even argue that the Huff et al. (2008b) call for a fine-grained IS/IT moral assessment and decision making instrument to assess IS/IT practitioners privacy understandings and knowledge is necessary.

Previously presented literature substantiates the conclusion that IS/IT practitioners' are committing privacy violations, and thereby not displaying exemplary computing behaviors. However, Huff et al. (2008a, 2008b) suggests that computing moral exemplars are not likely to commit privacy violations to PII because of their virtuous prosocial behaviors, and personal dispositions that preserve happiness and well-being in themselves and others. Walker and Frimer (2007) also substantiate this conclusion, because in general, exemplars display patterns of caring for others, as well as demonstrate morally relevant skill-set behaviors that are in accordance with RSOs. This

is not to say that every decision made by computing moral exemplars is of high moral impact, or even moral (Huff, Gassedeln, Gaker, Irvin & Payne, 2011). However, research into exemplars' behaviors and their sense of self do indicate a heightened sense of moral obligation in their work and life style, because "exemplars align their self-conceptions with ideal moral goals and personality traits, and their moral actions are undertaken as a matter of felt self-necessity" (Narvaez & Lapsley, 2009, p. 241). It therefore follows that based on the research of Huff et al. and others, that exemplars, especially computing moral exemplars are not as likely to commit privacy violations to PII due to their sense of a moral self. Based on this reasoning, computing exemplars represent the ideal theoretical group of comparison to determine if non-exemplar computing practitioners are more likely to commit privacy violations to PII.

If the PII privacy violation scale developed from this research demonstrates statistically reliable and valid data it will have the potential for application in the following manners. The instrument may aid organizations in appraising the moral decision-making capabilities for present, and potential new IS/IT employees about their abilities for handling privacy matters related to PII. Therefore, this new privacy assessment instrument could act as a gauge of trustworthiness. It also has the potential to act as a barometer indicating whether there is a need within the corporate environment for a Security Ethics and Training Awareness (SETA) program. The instrument could also serve as a tool by identifying some types and categories of PII privacy violations that need attention in corporate settings. Theoretically, if this new PII privacy violation instrument demonstrates statistical significance, it would be the empirical evidence supporting theoreticians claims that such an instrument is needed to identify what is lacking in the knowledge and understandings of privacy ICs and RSOs. Lastly, while not

conclusively being able to support all four of the PRIMES components, the instrument has the potential of validating some of the conclusions drawn from Huff et al. (2008a, 2008b), especially where the ICs and RSOs for PII privacy are concerned.

### **Barriers and Issues**

No discernable empirical literature appears to exist regarding today's Neo-Aristotelian virtues, computing practices, and IS/IT practitioners' moral reasoning and judgments. In addition, literature also appears to be almost nonexistent with regards to decision-making issues related to PII privacy except for the work of Kuo et al. (2007). Hence, little predictive literature indicates how to measure virtuous moral reasoning and its associated behaviors for privacy violations to PII. To resolve this, a new instrument was developed using aspects of Bebeau and Thoma's (1998, 1999) ICs, and Keefer and Ashley's (2001) RSO as they apply to IS/IT PII privacy. Because this was a new instrument acceptable levels reliability for the internal consistency of intercorrelated items of PII privacy violations was one of the hurdles that needed to be overcome.

Another barrier that this dissertation overcame was the requirement of validity in the ratings and rankings of the severity of privacy violations to PII. This was particularly important, because not all unethical behaviors are of equal severity. For instance, they can also be situation dependent (Calo, 2011; Chung & Khan, 2008; Lever, 2008), and cause different types of suffering as in psychological or financial harm (Nissenbaum, 2010; van den Hoven, 2008).

A further difficulty inherent to this research is that of the moral exemplar. Moral exemplar research has indicated that moral exemplar profile characteristics are not consistent across all situations (Huff, 2008a, 2008b; Walker, 1999, 2006). For example,



Hardy and Carlo (2006) mention that exemplars transcend boundaries in manners such as “different ages, races, gender, ethnic groups, and socioeconomic levels (p. 414).

Similarly, not all moral exemplars exhibit the same patterns of personhood. These types of variations in profiling make establishing a canonical list of exemplar behavior impossible, even though some exemplars do exhibit some centralized themes in their behavioral repertoires (Hardy, 2006; Hardy & Carlo, 2005a; Reed & Aquino, 2003).

Therefore, an all-inclusive personality profile for computing moral exemplars could not be distilled within the confines of this dissertation. Consequently, a limitation inherent to this research is the unintentional omission for some Hallmark Features, and demographic variables of the computing moral exemplar.

### **Limitations**

Due to the multidisciplinary breadth and depth of topics contained this research, an all-inclusive and exhaustive examination of every possible factor, construct, concept, model and theory is not possible, nor is it the intention of this dissertation to do so. The intention of this dissertation was an initial exploratory theoretical quantitative analysis to identify some of Hallmark Features, that interplay among IS/IT practitioners, and that are likely to affect their decision-making to commit or not commit privacy violations to PII.

Another limitation inherent to this research was that survey participants could have been influenced from their prior or current knowledge and understandings of organizational policies, or past ethics training. However, determining these effects on participant responses is necessary. Therefore, specific survey questions attempted to identify these factors of influence, and assess what if any effect they may have on study participants. Additionally, given the breadth of PII privacy violations, this study did not

attempt an exhaustive identification of all type of privacy violations that could be committed against PII. Rather, this research focused on intrusive PII privacy violations associated to the psychological, physical, and financial impacts that relate to concepts of identity theft and or fraud, but not necessarily be limited to them.

Due to the constraints of dissertation research, and the limited scope of this study, assessment of Social Desirability (SD) bias for study participant's responses was not a factor that was built into the survey design. Broadly understood, SD is the tendency for individuals' to deny the existence of undesirable personality traits in their character, in favor of traits that society views as favorable (Zerbe & Paulhus, 1987). In keeping with the Crowne and Marlowe (1960) SD Scale, moral exemplar personality characteristics are highly desirable, yet infrequently fully realized or displayed in society (Walker, 2006). Consistent with this line of reasoning, it is anticipated that single participant in this research would demonstrate total concordance with moral exemplary behaviors, and indicated absolute mastery of privacy ICs and RSOs. However, data screening measures were preformed to verify this.

While previously mentioned literature (Huff, 2008; Walker, 1999, 2006) addresses the issue that no canonical list can identify every characteristic of a moral exemplar, there are those (Hardy, 2006; Hardy & Carlo, 2005a; Reed & Aquino, 2003) who suggest that exemplars do exhibit some centralized themes in their behaviors. Therefore, an all-inclusive personality profile for computing moral exemplars is not realistic for the confines of this dissertation. Consequently, a limitation inherent to this research is the unintentional omission for some known or unknown personality factors of computing moral exemplars.

## **Delimitations**

Previously presented literature suggests that IS/IT practitioners commit privacy violations to PII. However, with no specificity have PII privacy violations been categorized by level of severity. Therefore, one of the objectives of this research was to create a PII privacy violations severity scale with the assistance of subject matter experts.

Variegated definitions of privacy cause ambiguities, and inconsistencies in the conceptualization and meaning of privacy (Solove, 2002, 2006, 2008). Likewise, IS/IT practitioners belonging to more than one IS/IT association may question which associations codes of ethics to follow (Abi-Raad, 1999; Oz, 1993). This is an issue when an IS/IT practitioners career necessitates multiple association memberships, and when the same ethical principle may be defined differently by two separate associations. Davis (2009) and the Center for the Study of Ethics in the Professions (2011) draw comparisons between various organizational codes of ethics, and entities such as privacy and respect, but here too the precision in definitional similarities are lacking. However, it should also be noted that the Association for Computing Machinery (ACM), and Institute of Electrical and Electronics Engineers (IEEE) formed a joint task force to develop a software engineering code of ethics. However, with only one branch of the ACM and one branch of IEEE joining in partnership, there continues to be a void between IS/IT organization's codes of ethics, which can cause ambiguities and inconsistencies for how concepts such as privacy and respect are represented. Similarly, Cordoba (2005), Gleason (2003), and Linderman and Schiano (2001) question the terminology and understandings of what IS/IT professionalism and socially responsible behavior is, and what precisely these words mean. While authors such as Linderman and Schiano, Oz (1992, 1993), Bower, Burmeister, Gotterbarn, and Weckert (2006), and Stahl and Wood

(2007) have attempted to define what computer professionalism is and is not, there remain numerous unanswered questions as to what *exactly* a computer professional is. To avoid issues associated with interpretive disparities of terminology, precise operationalized definitions are delimited in the Definitions of Terms section for this dissertation.

### **Definition of Terms**

For the purpose of this research, the following terms and definitions will apply:

- *Codes of Ethics* are sets of rules intended to guide the moral/ethical decision-making and behavior of individuals (Bricknell & Cohen, 2005).
- *Computer Ethics* is concerned with the principles, and standards of moral decision-making and conduct in the practice of good computing (Huff et al., 2008a 2008b).
- *Confidential Information* for the purposes of this research will represent a security state where information is secure, and not in jeopardy of disclosure to anyone not authorized to access it or use it (Boudol, 2009).
- *Deontology (Kantian) Ethics* represent the rights, duties, or obligations for rule-bound actions such as categorical imperatives that are not concerned with the goodness or badness related to the consequences of an action, but rather what one is supposed to do relative to a rule-based imperative obligations or laws (Hill, 2009).
- *Domain-specific Knowledge* is the exceptionally fine-grained conceptualization and understanding in professional codes of ethics that relate to a sub-category of profession-specific-knowledge (Keefer & Ashley, 2001).

- *Ethics* represents the systematic study and analysis of morality, by means of inquiry into of what we ought to do, and how we ought to think and behave (Darwall, 1998).
- *Identity Crime* centers on the misuse of PII for criminal activities (Jamieson et al., 2008).
- *Information Confidentiality, Assurance & Integrity* are defined for the purposes of this research as: confidential information is information that remains in the state non-disclosure and non-dissemination unless official authorization is granted. Information assurance and integrity unless otherwise stipulated refers specifically to the fact that the quality and context of all personal information remains constant to its original state and posture, unless authorization for modification and or dissemination has been granted by official sources.
- *Moral Agency of the Individual* is the ability and commitment to make explicit moral choices consciously and unconsciously that are morally self-regulating in relation to an object (Bandura, 2006).
- *Moral Exemplars* represent domain experts who exhibit virtuous behaviors within a particular field through their acquired procedural, declarative, and conditional knowledge (Narvaez & Lapsley 2005).
- *Moral Identity* is the degree to which virtues are central and important to one's identity (Hardy, 2006).
- *Morality* the commonly accepted and ascribed rules, norms, values, and laws that guide the behaviors of an individual, society, culture, or group of individuals (Donagan, 1977).

- *Personally Identifiable Information* Represents information used to distinguish or trace an individual's identity by the use of a person's name, social security number, biometric records, etc. (McCallister, Grance, & Scarfone, 2010).
- *Profession-specific knowledge* equates to Bebeau and Thoma's (1998, 1999) ICs. Profession-specific knowledge is morally relevant knowledge for the codes of ethics in a particular profession that come from training, mentorship, and experience. Profession-specific knowledge is a necessary precursor to Role Specific Obligations and moral decision-making.
- *Role Specific Obligations (RSO)* represent the mid-level or the profession-specific and domain-specific moral responsibilities attached to professional training and understanding, and are based on one's professional code of ethics (Keefer & Ashley, 2001).
- *Skill-sets* are the combination of recognizing moral opportunity and the ability to respond ethically to that opportunity through moral action (Huff et al., 2008b).
- *Social Responsibility* is defined for the purposes of this dissertation as the moral representation of care and respect for ICMs and their associated RSOs that aid in the protection to society's PII.
- *Teleological (Utilitarian/Consequential) Ethics* concerns itself with the consequences of behavioral actions, and stipulates that an action taken be for the greatest good for all (Audi, 2006).
- *Virtue Ethics* Unlike deontology or utilitarianism virtue ethics does not focus on a single act, but rather the character of the individual who does the right thing for the right reason, in the right ways at the right time, with honesty, compassion, fairness and kindness (Christie, Groarke, & Sweet, 2008).

## Summary

Studies directed at assessing IS/IT practitioner's decision-making choices towards the protection of PII appears to be almost non-existent. Given the dearth of empirical research in privacy violations to PII that are committed by IS/IT professionals, it becomes imperative to understand the IS/IT practitioners' personality profile in order to determine who may or may not commit privacy violations to PII. Therefore, this research will redress which IS/IT practitioners may or may not commit privacy violations to PII.

As has been demonstrated, today's IS/IT practitioners do commit privacy violations to PII (Cyber-Ark, 2009, 2010; Kuo et al., 2007). Immoral, illegal, and inappropriate behaviors within the field of IS/IT do lead to societal harm (Leonard & Cronan, 2001; Nissenbaum, 2010). Huff et al. (2008a, 2008b) suggests that IS/IT practitioners who exhibit at least some of the components of computing moral exemplars, such as the knowledge and understanding for ICs, and who act in accordance to their RSOs may be less likely to commit privacy violations to PII. Consequently, the need to determine which IS/IT practitioners are more likely to commit privacy violations to PII is paramount if the security to PII privacy is to be protected. However, not all violations to PII privacy carry the same level of psychological or economic harm (Chung & Khan, 2008; Nissenbaum, 2010; Solove, 2001, 2003, 2006). Therefore, the goals of this dissertation are to develop a new severity scale to measure PII privacy violations that are based upon the impact of psychological, or economic harm, and to determine if IS/IT practitioners are more likely to commit privacy violations to PII than are IS/IT computing moral exemplars. This newly developed instrument was administered to IS/IT practitioners, and currently stands as an independent measure with which to assess their decision-making behaviors towards committing privacy violations to PII. This

instrument will also serve as a measure with which to compare and analyze non-exemplar computing practitioners to computing exemplars.

The supposition behind this research is that because computing exemplars are believed to be highly moral and to be IC and RSO aware, they are less likely to commit violations to PII privacy. Should this research support the general suppositions, the instruments developed within this research may aid industry in choosing qualified applicants for IS/IT security jobs within organizations. Additionally, the new instruments developed for this research may also aid as a measure of awareness for security and privacy training within IS/IT security conscious organizations.

Three barriers need to be overcome to meet the requirements of this dissertation research. Given that, no preexisting methodology suggests how severity of privacy violations to PII should be measured, let alone rated, an expert panel will in part be enlisted for this purpose. Second, moral exemplar research is young, and was first developed in the early 1990s by Colby and Damon (1992). This means that only limited experimental data is available to draw upon for this dissertation. While others have called for moral assessment measures for the field of IS/IT (Woodward, 2007; Woodward & Ashby; 2006; Woodward, Davis, & Hodis; 2007), it is only Huff et al. (2008b) who have suggested that IS/IT moral assessment first be based on measures of privacy. Lastly, no canonical list exists that establishes a static personality disposition, or all inclusive hallmark feature set for all moral exemplars (Colby & Damon; Huff, 2009). Therefore, this research was designed to identify which IS/IT practitioners are willing to commit privacy violations to PII, given varying levels of severity to PII privacy violations.



## Chapter 2

### Literature Review

#### Introduction

According to Hovorka, Germonprez, and Larsen (2008) a major objective in research is to develop explanations from observed phenomena. Therefore, this literature review identified and examined previous literature that laid a foundation for how to best study the problem of IS/IT practitioner's privacy violations to PII, from the perspective of computing moral exemplars Hallmark Features. Additionally, behaviors, decision-making characteristics, and various demographic and life-style markers of moral exemplars were analyzed. Research methods are examined, and current gaps in knowledge are presented. Also addressed is how this dissertation fits within the broader context of IS/IT practitioners willingness to commit privacy violations to PII. Central to IS/IT practitioners willingness to commit privacy violations to PII, is the understanding of why computing exemplars are not as likely to not commit these types of violations. By understanding the good behaviors of computing exemplars, one is better able to identify unethical behaviors in computing. To accomplish this, this literature review pulls from exemplar literature in the fields of moral philosophy, moral psychology, moral development, and moral ecologies. In particular, by understanding these influences relative to exemplars Hallmark Features, one is better able to explain what feature components might be missing from non-exemplar IS/IT practitioners that would allow them to commit privacy violations to PII. Specifically, by examining, the moral philosophy and moral psychology of moral exemplars, a framework and methodology was built that permitted this study to compare the theoretical orientation of moral

computing exemplars against non-exemplar computing practitioners, and assess non-exemplar computing practitioners who were less willing to commit privacy violations to PII.

One framework proposed for understanding moral decision-making and moral behaviors in computing is virtue ethics (Huff et al., 2008a, 2008b; Volkman, 2004). For instance, Volkman suggested that classical virtue could help in “the spirit of the profession” (p. 2), while Huff et al. (2008a, 2008b) developed a theoretical model around virtue ethics that explains the moral performance of computing exemplars. Additionally, virtue theory provides a statistically validated framework in which character strengths, that is to say personality traits, dispositions, and Hallmark Features of exemplars neatly correlate with Neo-Aristotelian virtues (De Raad & Van Oudenhoven, 2011; Niemiec, 2013; Peterson & Seligman, 2004). However, there is more to understanding ethical decision-making and moral behaviors in computing than virtue ethics. Therefore, integrating philosophical perspectives to create compelling empirical evidence requires substantiated psychological realisms that are evidenced in reliable and valid research from fields such as moral development, personality theory, and moral ecology theory, which this dissertation heavily relied on.

Research over the past two decades has suggested a cohesive multi-domain and multi-pluralistic interpretation of personhood in order to understand and explain the self, the self’s moral development, and the self’s cognitive and behavioral systems (Narvaez & Lapsley, 2009a), this is particularly true when discussing moral exemplars and their virtuous behaviors (Frimer & Walker, 2008; Narvaez & Lapsley). Illustrating the depth and complexity needed to understand moral exemplars, Walker and Frimer (2007) noted that in order to obtain an encompassing profile of exemplars, one should examine

dispositional traits, characteristic adaptations, and life narrative stories; this line of reasoning is also consistent with Huff et al. (2008a, 2008b) and Huff and Barnard (2009). This multi-pluralistic interpretation of personhood represents a major shift in moral psychology, where in the past, streams of research primarily focused on singular elements of personality, such as trait theory, or behaviorism (Frimer & Walker; Narvaez & Lapsley). It is important to note that a full and rich historical body of literature supporting articulated ideas and statements made in this literature review may not meet with substantiated statistical evidence due to limited, yet expanding knowledge of moral exemplars. However, this is not to suggest that empirical evidence supporting the pluralistic understandings of moral exemplars does not exist, but further empirical research is required. For instance, Walker, Frimer, and Dunlop (2010) supported this line of reasoning by stating:

Empirical research with moral exemplars is relatively sparse because such samples are, by definition, uncommon. Early findings from qualitative analyses of moral exemplars (Colby & Damon, 1992; Monroe, 2002; Oliner, 2003; Oliner & Oliner, 1988) provided some conceptual insights, but the methodological limitations of such studies (lack of objective measures and appropriate comparison groups) constrain any definitive interpretation. (p. 911)

However, drawing logical conclusions based on current theoretical thought and applied findings is possible. Although given the dearth of current literature surrounding exemplars some anecdotal conclusions should be expected. It is, therefore, best to view this literature review and the methodology contained within this dissertation, as a deliberately descriptive exploratory investigation that synthesizes present postulations based on current theory of exemplarity, with statistically demonstrated evidence.

Even though research suggests multi-pluralistic examinations of moral exemplars in order to understand their self-systems and their behavior, the approach taken in this dissertation was limited to predicting moral and immoral decision-making of IS/IT practitioners behavioral intentions towards PII privacy, and comparing the results to the applied and theoretical understandings of moral exemplars and computing exemplars. Therefore, the following streams of research are present in this literature review but are not solely limited to them. These streams include moral philosophy, virtue ethics, moral exemplars, and computing moral exemplars. Also presented in this literature review is an examination of exemplar personality, how exemplars integrate morality into their self-system, their moral ecologies, their skills and knowledge, and various demographic variables, that when combined represent a framework for understanding moral decision-making and the ethical behavior of moral exemplars. By understanding the moral exemplar in these manners, we are then able to identify some of the variables that may lead to non-exemplary decision-making and behavior towards PII privacy. When combined these interdisciplinary fields form a framework in which to assess the ethical and unethical decision-making behaviors of IS/IT practitioners relative to privacy violation towards PII.

Privacy violations committed against PII are a human problem, not solely a technological issue. PII privacy violations are considered a problem, due to the high regard, and normative ethical values that society places on its privacy and PII (Hartshorne, 2010; Nissenbaum, 2010; Stahl, 2007). It is likely that the high regard that individuals hold for personal privacy comes from the internal values that they hold for the most confidential, sensitive and intimate information about themselves (Nissenbaum, 2004), and the uncontrolled ability to harvest personal information electronically

(Nissenbaum, 1998; Tavani, 2005). Literature also substantiates that those empowered to protect society's digital PII, namely IS/IT practitioners, are in some instances the very individuals committing privacy violations to PII (Cyber-Ark, 2008a, 2008b, 2009, 2010, 2011; Kuo et al., 2007). Most privacy violations are considered unethical, though they do not all rank at the same level of severity (Chung & Khan, 2008). Nonetheless, all PII privacy violations have the potential to cause psychological and financial harm (Holtzman, 2006; Moor, 1990). Stated with some certainty, studies directed at identifying those IS/IT practitioners that are likely to commit privacy violations to PII appear to be almost non-existent. Therefore, the purpose of this dissertation was to determine which IS/IT practitioners were less willing to commit privacy violations to PII based on their comparative Hallmark Features of the Huff et al. (2008a 2008b) computing exemplars. It is theorized that those IS/IT practitioners that score higher on the Hallmark Features of moral and computing exemplars, will be less willing to commit privacy violations to PII, than are those practitioners that score lower on said Hallmark Features.

### **Moral Philosophy**

Normative ethics provides a foundation, and a structure that allows a discourse and the ability to determine morally right and wrong behaviors when discussed in terms of deontological or consequential ethics. In its simplest terms, we can look at these two forms of ethics as either principled rules of universal moral obligation or duty, as in the Kantian categorical imperative, or the utility of consequences, such that, actions should maximize over all happiness, as in Bentham's and Mill's account of utilitarianism (Audi, 2006; Bartels, 2008; Singer, 2008). As such, both forms of ethical theory and inquiry offer different and competing axiomatic principles that state how we should analyze

ethical dilemmas, and make ethical decisions. While both represent psychological processes used in moral reasoning and decision-making (Reynolds, 2006; Shanahan & Hyman, 2003), a noted difficulty associated with both of these schools of thought is that they lend themselves to both relativisms and rationalizations (Volkman, 2004). More precisely, Volkman suggests that when confronted with an ethical dilemma that requires resolution, rationalizations that justify the relative situation are easy to rely on. Volkman goes on to say that both of these systems operate in the “one’s self-interest” (p. 3). A further shortcoming found in both deontological and utilitarian ethics is the focus on what one *ought to do*. Alternatively, a virtue-based approach to ethics concentrates on the act of an individual doing the right things, at the right time, for the right reasons (Nisigandha, 2007; van Zyl, 2009). Virtue theory delineates what it is for an individual to have virtue(s) of character, or the excellences within one’s self, instead of predetermining what one should do based on a sets of rules, duties, or consequences, as is the case in deontological and utilitarian ethics. In particular, virtue theory asks and attempts to answer a myriad of questions that revolve around a person’s character, rather than how situations should ethically be resolved. These questions are epitomized in the following manner; what does it mean to be good, how does one become good, what kind of person should I be, and how should I live (Athanasoulis, 2010). As such, virtue ethics is not constrained by the limitations of deontology and utilitarianism.

### **Virtue Ethics**

In *Nicomachean Ethics*, Aristotle (1999) puts forth the opinion that true happiness results from a virtuous life. To this, he adds that virtue is a state between 12 means that sit between excesses and deficiencies (Appendix A). For instance, the virtue of courage

sits between the excess of rashness and the deficiency of cowardice. Aristotle also claims that a person cannot possess one virtue without possessing all other virtues (Telfer, 1989). However, understanding neo-Aristotelian virtues, and virtue to trait characteristics paint an altogether different picture. Hursthouse (1999) shares a common belief among neo-Aristotelian virtue ethicists that, virtues are necessary in order for happiness to flourish. Hursthouse also suggests that virtues must benefit the possessor, and that virtues make the possessor a good human being, this is similar to Aristotle's view of what is necessary for a purposeful life (Aristotle, 1999). However, Hursthouse notes that neo-Aristotelian ethicists do not limit themselves to Aristotle 12 virtues. An examination of Appendix B provides evidence of other virtues that appear in the fields of moral development, moral identity, moral exemplar, and personality research (De Raad & Van Oudenhoven, 2011; Hardy, 2006; Narvaez & Lapsley, 2009a, 2009b; Walker, 1999, 2004; Walker et al., 2010). While Appendix B provides a listing for some of the more frequently cited virtues in literature, one recurrent finding among virtue research bears explanation. Shanahan and Hyman (2004) note that certain virtues fall into groupings. Their research found significant correlations around six virtues. The six factors were empathy, protestant work ethics, piety, reliability, respect, and incorruptibility. Once broken down and analyzed it was found that empathy clusters around the virtues of compassion, caring, graciousness, attentiveness, amiability, generosity, humility, trust, and contentment. Similarly, the protestant work ethics clustered around virtues such as creativity, passion, competitiveness, ambition courage, and the like. When examining piety, the authors found that saintliness and spirit also related. Additionally, reliability clustered with responsibility, trustworthiness, ability, articulateness, and prudence. Lastly, respect clustered around cool headedness, tolerance, and cooperativeness, while

incorruptibility clustered with honor, honesty, and integrity. Murphy (1999) provides further support for the notion of neo-Aristotelian virtues converging when he posited that at least five core virtues and six related virtues are identifiable in the field of international marketing (Appendix C). What these two pieces of literature demonstrate is that virtues do not stand in isolation to one another. However, what these literatures do not explain is, how personality traits relate to virtues, or how virtues and traits related to moral functioning and decision-making.

Previous decades of literature on virtue, character strengths, and personality traits indicate that these constructs were often treated as individual factors of influence on decision-making and behavior (Allport, 1927, 1961; Cattell, 1946; Eysenck, 1970; see also Cawley, Martin & Johnson, 2000; Digman, 1990; Peterson & Seligmann, 2004). Realizing the need for a more comprehensive framework that explains personality McAdams & Pals (2006) proposed the following:

...as (a) an individual's unique variation on the general evolutionary design for human nature, expressed as a developing pattern of (b) dispositional traits, (c) characteristic adaptations, and (d) self-defining life narratives, complexly and differentially situated (e) in culture and social context (p. 204).

For example, this framework now allows once isolated constructs such as altruistic prosocial behaviors, communion and agency, and religion and spirituality to more easily integrate with the virtue constructs found in exemplar research (Frimer, Walker, Lee, Riches, & Dunlop, 2012; Walker & Frimer, 2007, 2008, 2009; see also Bebeau, 2008; Bebeau & Monson, 2008; Mastain, 2007). In addition, by adapting this multi-domain multi-pluralistic framework Huff et al. (2008a, 2008b) were able to develop the theoretical model of PRIMES that is capable of explaining good computing behavior by



examining exemplars personality, their integration of morality into a self-system through life narratives, their moral ecologies of social context, their expert knowledge and skills.

### **Moral Exemplars**

Neo-Aristotelian virtues manifest in exemplar's psychological processes and behavioral tendencies towards moral action (Narvaez & Lapsley, 2009a), therefore, when combined, we can label these processes and tendencies as exemplars' dispositions. These moral dispositions represent compositions of personality traits and characteristics, the integration of morality into a moral self-system, influences from environmental ecologies, and moral skills and knowledge that when combined facilitate exemplar ethical action that is a projection of one's moral self to the self and to society (McAdams & Pals, 2006; Narvaez & Lapsley, 2009a; Walker & Frimer, 2007). More precisely, exemplars live a life where there is a "unity between their sense of morality and their personal goals" (Hardy & Carlo, 2011a, p. 213). Thus, it is logical and correct to say that excellences of virtue or exemplary moral behaviors are not possible "without concrete activity" (Richardson, 2012, p. 27). Holistically, exemplars represent relatively stable dispositions of personhood that develop over a lifetime, and that become embedded within who they are, when continuously nurtured by mentorship and their environments (Athanasoulis, 2010; Huff et al., 2008b). An example of these relatively stable dispositions is present in exemplar acts of kindness. For instance, once embedded, kindness is exhibited across exemplars' life events unless a situation requires otherwise. Similarly, a computing exemplar that exhibits a respect for individual's privacy is likely to do so across most situations. Because of this life-long tendency towards kindness and respect for privacy, it may also be said that the dispositions of kindness and respect are

somewhat fixed characteristics of the exemplar. Additionally, exemplars also act with the intent to do right (Ryan, 1998), and do so in order to remain true to one's self (Williams & Murphy, 1990). According to Christie, Groarke, and Sweet (2008) true virtue is, "...do the right thing, to the right people, at the right time, in the right way, for the right reasons" (p. 56).

Among others, Narvaez (2008), Narvaez and Lapsley (2005), Walker and Pitts, (1998), and Walker (1999) indicate that procedural, declarative, and conditional skills and knowledge allow exemplars' to become domain-specific moral experts, such as in the case of computing exemplars. It is also their moral skills and knowledge that gives them the capacity towards sustained moral actions, which is represented in their abilities to integrate a working mastery of ethical sensitivity, ethical judgment, ethical focus, and ethical action (Narvaez, Bock, Endicott, & Lies, 2004; Narvaez & Lapsley, 2005). It is because of this mastery that they can take their skills and knowledge of ICs, and transfer them into domain-specific ethical actions of RSOs.

**Exemplar moral development.** Literature is replete with moral development stage theories that describe ethical reasoning and decision-making (Gilligan, 1982; Kohlberg, 1969; Piaget, 1932; Rest, 1986). However, Rest's (1979, 1986) four-component model of moral development is the one most often cited in today's literatures (Xu, Iran-Nejad, & Thoma, 2007), and the one that best describes moral development in exemplars, because it is also capable of accounting for virtuous actions. Among other notable items, Rest's (1979, 1986; see also Rest, Thoma, & Edwards, 1997) four-component model describes how exemplars' move back and forth between stages. The model also accounts for the cognitive and affective elements of moral development by

highlighting moral reasoning and decision-making using the components of moral sensitivity, moral judgment, moral motivation, and moral character (Rest, 1979, 1983, 1984, 1986).

The following explains how these components manifest in exemplars. Moral sensitivity entails an interpretive awareness of situations, recognition of how actions affect others and the ability to use imagination to create scenarios so that others' feelings are considered (Lincoln & Holmes, 2011; Walker, 2004). Therefore, moral sensitivity requires sympathy and empathy (Bergman, 2002), which are mainstays of moral exemplar's dispositions (Carlo, Hardy, & Alberts, 2006; Colby & Damon, 1992; Walker & Henning, 2004). Without moral sensitivity, depth of insight would be lacking, thus creating shortsighted emotional perception. Moral judgment is the ability to deliberate ethically about what is right and wrong from multiple perspectives (Monson, 2009); it is akin to the formulating and assessing ethical solutions that are morally justified. Additionally, moral judgment, especially for exemplars, entails learned components of ICs and RSOs (Bebeau & Thoma, 1998, 1999; Keefer & Ashley, 2001). Blasi (1999) maintains that to behave with moral motivation is an intentional and conscious process. Rest (1986) defined moral motivation as the ability with the intention to "prioritize moral values over personal values" (Bebeau, Rest, and Narvaez, 1999, p. 22). It is in this third component that the moral individual is deciding to act, and therefore, fulfill the moral ideal through an ethical course of action (Myyry, 2003). Rest's fourth component, moral character, requires having the courage, conviction, determination, and skills necessary to carry out an ethical action, even in the face environmental pressures. For this reason, Walker (2004) remarked that; it is in this stage that the individual "engenders effective action" (p. 553). However, if an individual does not possess the capabilities required in

this stage of moral development, moral behavior fails, because moral character requires the ability to be self-disciplined, and control impulses (Bebeau, Rest, & Narvaez), as well as the skills and knowledge necessary to carry out the ethical behavior.

**Exemplar influences.** Rest's (1979, 1986) four-component model gave rise to new literatures and understandings that helped to explain the development of the moral self. Many of these developments took place in four specific areas. These areas have come to represent four individual, yet recurrent and stable moral exemplar domains of influence that orchestrate in concert to represent much of the wholeness that comprises exemplar personhood. Each of the four influential areas that comprise the exemplar, that is to say, personality, the integrated self-morality system, social surrounds, and moral skills and knowledge, are necessary, but not individually sufficient to explain the moral exemplar (Huff et al., 2008a, 2008b). It is the totality of these areas, and their cohesive psychological processes and functions that allows for a more complete distillation of the moral exemplar to surface. In some instances, components of these areas also represent partial schemas of the exemplar. It is also through these schemas of who and how they are, that their lives come to positively affect those around them, and the world as a whole. Loosely defined, schemas can describe thought and behavior patterns, and provide a framework for understanding cognitive processes and behaviors (Narvaez & Bock, 2002). Additionally, schemas represent knowledge structures that reside in long-term memory, and that support information processing (Rest et al., 2000; Walker, 2002b).

**Personality.** Personality psychology has demonstrated that early in a person's development traits take hold, and are mooring points for behavior. These traits are also

determinants of behaviors. Of all four influencing areas, personality traits display the least amount of malleability. This is not to say that one's social surrounds (Huff et al., 2008a), and stage in life (Roberts & Mroczek, 2008; Roberts, Walton, & Viechtbauer, 2006) are not capable of influencing behavioral traits in one direction or the other. One of the most noted and used personality trait scales is the Big-Five, which measures openness, conscientiousness, extroversion, agreeableness, and neuroticism (Walker & Henning, 2004). Literature examining the Big-Five and exemplarity has found that every trait other than neuroticism correlate with moral exemplars' personalities (Matsuba & Walker, 2004; Walker & Henning; Walker & Pitts, 1998). More recent findings indicate that as individuals age, they demonstrate higher degrees of agreeability and conscientiousness (Lucas & Donnellan, 2009), and become more emotionally stable (Roberts et al.). Roberts and Mroczek also maintain that with increased age comes gains in self-confidence, greater self-control and that individuals display more warmth. Nevertheless, even as strong as personality traits are in a person's life, they are not the sole determinants of ethical decision-making and behavior (Huff et al., 2008a).

As previously discussed, McAdams and Pals (2006) developed a new and promising framework in which to understand personality that was based on the original Big-Five Trait Theory. The significance of their approach was that it retained the elements of personality trait theory, but it also acknowledged that traits alone were not enough to fully understand, appreciate, or assess individuals. What McAdams and Pals did was to articulate five principles that when added to the original Big-Five traits, created a more integrated and cohesive understanding of the whole individual that is inclusive to exemplars (see Virtue Ethics section). Even with the relative stability of personality traits, and the McAdams and Pals integrative paradigm, it is necessary to

understand that personality traits are but one component of the moral exemplar, and that taken individually traits do not, nor can they provide a detailed representation of who the moral exemplar is.

*Integration of morality into a self-system.* Exemplars integrate morality into a self-system. Blasi (1980, 1983) and Hardy and Carlo (2005a, 2011a, 2011b) developed new insights into how individuals integrate morality into a self-system through their senses of moral commitment to themselves and society. Their literatures also provided insights for why and how individuals act with a sense of morality. For example, Huff and Frey (2005), noting Blasi (1980), argue that is not just how exemplars integrate moral judgment, moral commitment, and principles into their self-concepts, but that they do so in the fundamental sense of their self-image. Huff and Frey further suggest that if moral exemplars denied this tightly woven fabric of their moral self-image, it would represent a denial of who they truly are. Likewise, Colby and Damon (1992) recognized, as did Blasi (1980, 1983), McAdams (2006), and McAdams et al. (2008) that exemplar's moral commitment was essential to their sense of self, and that when fostered by their environments, this integration of morality into the self-became deeply embedded into their life stories, and their moral commitment to society.

It is through the exploration of exemplar's moral judgment, moral commitment, moral principles, and social responsibility that we also see the connection between the self and principles. In their analysis of moral exemplars, Schlenker, Miller and Johnson (2009) depict the connection between self and principles through exemplar's feelings of obligations to moral principles, and by stating that these feelings "have been both internalized and appropriated as part of one's identity" (p. 319), and as such, this means

that principles, ethical values, and rules are now looked upon as “moral convictions that are ‘owned’ by the self and that guide behavior” (p. 319). Simply put, it is in part due to this interconnection that exemplars represent the highest standards in moral excellences both personally and professionally, and contribute to society in ways that increase human flourishing. Additionally, while it is necessary to understanding how the integration of morality into a self-system works for the moral exemplar, it is not sufficient because it is only but one of many parts that comprise the exemplars disposition.

***Moral ecologies.*** Organizations are the social actors of their employee’s value systems (Victor & Cullen, 1998); therefore, they represent the moral and immoral behaviors of their employees (Trevino, Weaver, & Reynolds, 2006). It is within these social ecologies that decisive moral and immoral decision-making takes place. In these social surrounds, the exemplar interacts in a web of interconnected communities. Moral ecologies, no matter how stable, require constant negotiations because of the interacting influences found in organizational values, societal pressures, and community and family expectations (Brinkman 2004; Huff et al., 2008b). Because of this variability, Aquino, Freeman, Reed, Lim, and Felps (2009), and Huff et al. (2008b) note that social surroundings either promote or circumvent ethical actions. Moral mentors, professional organizations, and religious affiliations are all representative examples of social surrounds that can help promote ethical decision-making and moral behavior. When a moral ecology promotes exemplar’s actions, the social surrounds provide a meaningful world with moral components where exemplars have purpose and reason for ethical action (Brinkman; Huff et al., 2008a, 2008b).

Because organizational ecologies are capable of exerting influential forces upon a person, knowing how to negotiate these surrounds is often a matter of whether or not the exemplar can have a positive lasting effect within a social surround. In effect, moral actions within organizational social surrounds are critical to understand because they can and do influence IS/IT practitioner's ethical decision-making skills and behaviors. Some of the items that exert influence on exemplars in their organizational environments are organizational structures, codes of ethics, and ethics training.

*Organizational structures.* Two often-cited organizational structures are mechanistic and organic, and they both ascribe to distinctly different patterns of ethical behavior (Jin & Drozdenko, 2003, 2010; Jin, Drozdenko, & Bassett, 2007; Jin, Drozdenko, & Deloughy, 2010). Among other salient factors, values of organic organizations characteristically promote social welfare and social responsibility by fostering ethical values, they openly encourage creativity and collaboration, and are empowering towards their employees (Jin & Drozdenko, 2010; Jin et al., 2007). These organizational hallmarks support and promote exemplary type behaviors because, like the exemplar; they promote social welfare. By contrast, mechanistic organizations represent and value ridged hierarchical lines, which are task oriented, less opened-minded, and have a capacity towards less principled behaviors then organic organizations (Jin & Drozdenko, 2010; Jin et al., 2007). Research conducted with IS/IT practitioners in both mechanistic and organic valued organizations confirms that organizational social surrounds either promote or hinder ethical behavior (Jin et al., 2007).

Jin et al. (2007) found strong supporting evidence that IS/IT workers employed in mechanistic organizations reported significantly higher perceived levels of unethical



behaviors than those in organic organizations. Furthermore, even with the higher levels of managerial oversight that is inherent within mechanistic organizations, this oversight was not a factor in suppressing perceived unethical behaviors. Following Jin et al. (2007), Jin and Drozdenko (2010) postulated that IS/IT practitioners working in organic-based organizations reported higher levels of social responsibility in their organizations. The author's interpretation for this was that organic organizations encourage "community service projects and activities" (p. 349), and that there appeared to be a focus on social responsibility that goes "beyond the interest of shareholders" (p. 349), and that top-level managers support values such as compassion and helping. Secondary to their first hypothesis, Jin and Drozdenko postulated that: "IT professionals working in organizations that are more socially responsible are also more ethical" (p. 349). Here too the results proved significant. The importance of this finding is that organic-based organizations likely possess higher levels of moral reflection, which is consistently a characteristic found in moral exemplars (Blasi, 1983; Hardy & Carlo, 2005a, 2011a; McAdams, 2006). Therefore, it is a logical endeavor to determine if those IS/IT practitioners that identify their organizations as supporting social welfare are not willing to commit privacy violations to PII.

*Codes of ethics and training.* Corporate ecologies use codes of ethics to curb unethical behaviors (Kaptein, 2011), and promote the moral health of the organization by formally encouraging responsible behaviors (Rodriguez-Dominguez, Gallego-Alvarez, & Garcia-Sanchez, 2009). Codes of ethics also help to resolve information systems ethical dilemmas (Singh, 2011). To date, Harrington (1996) provides the most convincing evidence that codes may help in decision-making processes related to IS/IT practitioner.

While Harrington found no effect for *general codes of ethics* among IS/IT practitioners, *specific codes* related to computer abuse did demonstrate a positive effect. Among other notable findings Harrington's data indicated that an individual's traits are likely to play a mediating role in decision-making, and individuals' who would already assume positive responsibility for their actions were only minimally influenced by codes of ethics. Lastly, Harrington found that codes are likely to have more effect for those individuals who had a propensity to deny responsibility. The idea of owning responsibility is of critical importance to Harrington's study. It supports the notion that individuals such as moral exemplars, who already assume moral responsibility, have developed the skills and knowledge through various environmental influences to make ethical decisions (Moberg, 2000). Therefore, it makes sense to determine if those IS/IT practitioners that are aware of their company's IS/IT codes of ethics, are not willing to commit privacy violations to PII.

This is not to suggest that an organizational code of ethics program or IS/IT security and privacy awareness program is going to turn a non-exemplar computing practitioners into computing exemplars. However, evidence suggests that skills and knowledge of moral responsibility can be taught through ethical awareness programs, and that these programs produce ethical decision-making and ethical behavior not only in the organizational setting (Frisque & Kolb, 2008; Sekerka, 2009), but also for professional practitioners (Bebeau, 2009a, 2009b). Furthermore, these types of educational training programs also instill moral understandings for ICs and RSOs (Bebeau, 2008; Bebeau & Thoma, 1998, 1999; Keefer & Ashley, 2001). Evidence from Bebeau (2008, 2009a, 2009b) and Bebeau and Thoma suggests that those individuals taught to understand

ethical conceptualizations of morality in relation to their ethical RSOs, consistently make better and more accurate ethical decisions.

Additionally, non-compliance with IS/IT policies, which includes privacy violations, are a major concern for organizations (Karjalainen & Siponen, 2011). Zimbardo (as cited in Sekerka, 2009) asserts that given the correct context moral individuals uncharacteristically will transform and engage in “unethical decisions and acts” (p. 94). One commonly employed approach to improving unethical IS/IT decisions and behaviors are to employ an employee awareness-training program (Puhakainen, 2006; Zumrah, Boyle, & Fein, 2012). Furthermore, research supports a positive relation between organizational ethical awareness training, conformity to organizational codes of ethics and ethical decision-making (Stevens, Steensma, Harrison, & Cochran, 2004). Lastly, Harrington (1990) maintains that an ethical awareness program for IS/IT related issues may actually reduce IS/IT ambivalence to ethical issues. This is significant because training is a source of mentorship, and exemplars cite mentors as one of their driving forces in their moral education (Huff et al., 2008b). Based on this knowledge, one question that this research will explore is, are those IS/IT practitioners who have had exposure to ethics training not willing to commit privacy violations to PII.

The above discussion on moral ecologies suggests that they are likely to have an effect on exemplars and ethical decision-making. However, it is necessary to understand that moral ecologies singularly are not sufficient to explain exemplar dispositions or functionally respective to solely explain ethical decision-making and ethical behavior. Among other factors, moral skills and knowledge also play a pivotal role in influencing ethical decision-making and moral behaviors.

*Moral skills and knowledge.* Computing exemplars' decision-making and virtuous behaviors require specialized virtue skills and knowledge in order to sustain their moral actions (Huff et al. 2008a, 2008b, 2011). It is through the understanding and use of ICs and RSOs that computing exemplars are able to display profession-specific technical competencies, with an emphasis towards moral action that is other-centered, rather than self-centered (Bebeau, 2008; Huff et al. 2008a, 2008b, 2011). This implies that computing exemplars can bring their behavior under the "explicit guidance of rational deliberations" (Narvaez & Lapsley, 2005, p. 141), as in self-reflection. This is consistent with Bandura's (1991a, 1991b, 1999a) self-efficacy, and Blasi's (2005; see also Lapsley & Hill, 2009) conceptualization of willpower (alternatively, self-control), which is considered a moral skill that enables and promotes ethical decision-making and moral behaviors.

Blasi (2005) describes self-control as a clustering of two higher-ordered virtue skill sets comprised of traits, and one lower-ordered virtue skill set of traits (Huff et al., 2008b; Lapsley & Hill, 2009), that can be understood as an exemplar's dispositional or personality trait "toolbox" (Lapsley & Hill, p. 197). For Blasi (1983) these ordered virtue skills (Appendix D) represent the individual's moral self-responsibilities. From this toolbox, exemplars self-govern and sustain moral action in matters of ethical decision-making and morally right behaviors. Among other items, Blasi's (2005) virtues toolbox helps to explain how computing exemplars dispositions find form and function in skills such as, self-accountable, being true to oneself, and resistance to self-deception. It is with these virtues and skills that exemplars transform the practice of virtue skills and behaviors into life-long dispositional embedded virtue habits. Due to their commitment towards virtue skills and knowledge, their moral actions are displayed in their ability to

identify when ethical issues arise and when ethical responses are required (Bebeau & Thoma, 1999); therefore, they are capable of resolving ethical dilemmas with sound ethical decision-making (Bebeau & Thoma). However, this toolbox is only one component that sets moral exemplars apart.

Like Rest (1983, 1984), Narvaez (2005, 2006, 2008) maintains that the moral skills and knowledge of a domain-specific experts requires nothing less than effectively “developing appropriate intuitions and sophisticated deliberations in at least four areas” (p. 318-319). These four areas are ethical sensitivity, ethical judgment, ethical focus, and ethical action (Appendix E), and all require certain virtue skills like those listed in Appendix D. Additionally, with continued practice these skills become routinized within the exemplar (Narvaez & Lapsley, 2005). These routinized skills suggest that conscious moral deliberation may not be required for ethically sound decision-making, because decision-making becomes automatized, at least in part due to internal situational awareness’s, which is what helps to drive morally appropriate actions. For Blasi (1980) the link between moral motivation and moral action lies in the explicit nature of an individual staying consistent to their moral integrity, such that, an action is not only seen as moral, but that it is morally right for the exemplar. This suggests that moral actions are rooted in a person’s moral emotions, which tie to moral self-regulation (Blasi, 1999, 2005).

The common thread running between Blasi (1999, 2005) and Narvaez (2005, 2006, 2008), is that Blasi’s self-model requires an internal situational awareness for moral self-responsibility, while Narvaez’s four-process model requires an external moral situational awareness. Therefore, it can be said that both the internal and external situational awareness provide motivation for exemplary moral decision-making and

ethical behaviors. Of particular note is how Narvaez, Bock, Endicott, & Lies (2004) and Narvaez and Lapsley (2005) find commonality with Rest's (1983, 1984) four-component model. Narvaez et al. reasoned that moral skills (alternatively virtues) could be cultivated through education to high-levels of expertise, as one might train, mentor, and cultivate the skills of an apprentice and thereby make the apprentice a morally knowledgeable expert; this is akin to educating a moral novice to become moral expert with professional "know-how" (Narvaez & Lapsley, 2005, p. 154). Narvaez & Lapsley (2005), extended Rest's (1983, 1984) model by articulating a moral experts skills list that included a "set of social, personal, and citizenship skills" (p. 155) that could be used in moral education (Appendix F). The model took each of Rest's four components and added seven sub-skills to each of the four components, thereby creating 21 sub-components. Huff et al. (2008b) noting that the Narvaez and Lapsley (2005) research provided evidence that moral skills can be taught (alternatively mentored), also brought attention to the fact that Narvaez and Lapsley's (2005) discussion of moral motivation and ethical action lends itself to moral skill-set development with professional ICs. Therefore, by articulating moral skills in the manner that Narvaez and Lapsley (2005) did, and effectively cultivating these virtue skill-sets with mentoring and education, the moral novice moves closer to the high-level knowledge of ethical expertise and action that moral exemplar exhibits.

*Mentoring.* One identifiable characteristic of most moral exemplar's life narratives are the mentors that have influenced them, and how their social systems, such as work colleagues, friends, family, and religious affiliation all supported and promote their ethical actions (Colby & Damon, 1992; Huff & Rogerson, 2005; Walker & Pitts,

1998). What this suggests is that exemplars are in part learning their moral excellences from their moral ecologies, and that these ecologies are acting as mentors. Narvaez and Lapsley (2005) postulated that moral experts, conversely, moral exemplars, become experts in three distinct manners. First, experts learn from interacting with their environment, or direct education that has three characteristics: they learn from situations that “reward appropriate behavior” (p. 153), they transform explicit theory into tacit knowledge, and they focus on an immersive continual practice of skills. Second, they learn to implement implicit, explicit, and tacit skills and knowledge that previous experts in their profession developed. Lastly, they spend limitless hours of time-focused practice honing their moral skills and knowledge under the tutelage of established domain experts. Additionally, Narvaez and Lapsley note that moral experts have well organized declarative and conditional schemas, and that they possess expert decision-making capabilities that novices do not. Because of this, one can say that computing exemplars know what skills and knowledge to access when presented with domain-specific ethical dilemmas. Therefore, it is in part through their mentors, and environmental learning and education that computing exemplars begin to relate the ICs of their career domain to their RSOs of practice, thus allowing for purposeful moral action. It is because of the relationships that exemplars have with mentors that this research asks the following question: Are IS/IT practitioners not willing to commit privacy violations to PII if they identify that they have had moral mentors guide them in their careers?

*Intermediate concepts & role-specific obligations.* Moral and computing exemplars display domain specific ethical sensitivity, judgment, and the motivation to carry out ethical actions by activating ICs and RSOs that develop from their moral

schemas. Keefer and Ashley (2001) identified a distinct behavioral pattern of moral action that they labeled RSOs while studying domain experts. They noted that RSOs are the experts' ability to act with ethical professionalism within their domain of expertise. For computing exemplars, this would be analogous to not using consumers PII for marketing purposes because end-users of an Internet Web-based store opted out from allowing their information to be sold to third-party marketers.

Contributory to RSOs is the requirement of correctly identifying domain-specific ICs within the exemplars field of practice (Bebeau, 2008; Huff et al., 2008a, 2008b). To Bebeau and Thoma (1998, 1999), ICs represent the domain experts' cognitive representation and understanding of core ethical abstract conceptualizations that professionally bind them to their fields of practice. ICs act as ethical guidelines for moral decision-making, and as such aid the exemplars in their RSOs. Therefore, it stands to reason that with continued practice and time, ethical decision-making and behaviors are likely to increase as exemplars practice their RSOs relative to their domains ICs. This assertion aligns with the research of Huff et al. (2008a, 2008b), Muraven and Baumeister (2000), Neil, Wood, and Quinn (2006) Webb and Sheeran (2006) and Wood (2005) who have maintained the position that, virtues displayed as personal dispositions improve with practice. For example, computing moral exemplars that work in the field of information privacy would possess an internalized conceptualization for what privacy and informed consent means. Therefore, the longer a computing exemplar works with information privacy, the more embedded these ethical conceptualizations become, and the less likely they are to violate these conceptualizations of privacy and informed consent, because to do so would represent a break with their moral convictions.



**Other exemplar factors.** Schemas are powerful cognitive representations that exemplars use to process information, navigate their perceptions, guide decisions, and orient behaviors. While moral exemplars represent a composite of their four areas of influences and their schemas, a review of literatures identifies other dispositional attributes such as various Hallmark Features, and socio-economic factors that contribute to their personalogical makeups. Among other items, exemplars exhibit high levels of prosocial behaviors (Huff & Frey, 2005; Walker & Frimer, 2007, 2009), and are noted to integrate religion and spirituality into their lives (Hardy, Walker, Rackham, & Olsen, 2012; Walker, 2003; Walker & Frimer, 2008). Additionally, limited yet discernable literature discusses how the four influential areas, schemas, and the Defining Issues Tests (DITs) relate to exemplarity (Lapsley & Narvaez, 2006; Thoma & Bebeau, 2013; Williams, 2009). Both versions of the DITs, the DIT-1, and the DIT-2 are moral assessment instruments designed to activate an individual's moral schemas, and measure an individual's level of moral reasoning and moral maturity (Rest, Thoma, & Edwards, 1997; Rest, Thoma, Narvaez, & Bebeau, 1997; Rest, Narvaez, Thoma, & Bebeau, 1999, 2000). The DIT-2 is the update and shorter version of the DIT-1. High DIT scores represent higher levels of moral maturity, higher levels of education, and often individuals of more advanced age (Rest et al. 1978; Rest et al., 1999). Because higher DIT scores are also associated with higher levels of education, they are also likely to correlate with more advanced career positions. These factors and other are discussed in more detail below.

***Hallmark features.*** Moral exemplars are often cited for their altruistic prosocial personalities. Macaulay and Berkowitz (as cited in Jeffries et al., 2006) define altruism

as a state of “behavior carried out to benefit another without anticipation of rewards from external sources” (p. 3). This may also be interpreted as a goal-directed behavior meant to enhance or help others welfare. For instance, Oliner and Oliner (1998) documented the efforts of exemplars who exhibited a particular sense of societal welfare through their prosocial behaviors by rescuing Jews during WWII. Similar findings of prosocial helping behaviors among exemplary individuals have been noted by Hardy (2006), Huff et al. (2008a, 2008b), and Huff and Rogerson (2005). Hardy maintains that there is a positive relationship between prosocial identities, and how individuals see themselves in terms of caring and empathizing for society. In simpler terms, one’s prosocial identity predicts one’s prosocial behavior. For instance, the more one cares and empathizes for matters related to societal welfare, the more likely one is to act in a caring manner towards particular societal issues of personal concern. In like fashion, Huff et al. (2008a) and Huff and Rogerson identified two groups of exemplars noted for their prosocial agendas in the field of computing. Computing craftspersons design systems that aid individuals, while computing reformers work for and towards the betterment of society in the field of computing. This disparity between exemplar prosocial behaviors is common. In fact, literature suggests that even though exemplars share similarities, their personality profiles take on “multifarious forms” (Walker & Frimer, 2007, p. 859). One explanation for these personalogical differences may be how the four influential areas and schemas of exemplarity develop and play out in each exemplar. This is supported by Huff and Rogerson (2005) who point out, when compared to computing reformers, computing craftspersons are unique among exemplars “because the values they hold are already intrinsic to computing and their skills are intertwined with, and depend upon, technical expertise” (p. 5). Likewise, Huff and Rogerson note that craftspersons display a more

optimistic affective tone in their life stories than do reformers. One explanation for this difference is that reformers more often have to deal with societal roadblocks. This type of commonality and divergence of exemplar personality and disposition is common in other areas of their lives too.

Literature is replete with anecdotal and empirical evidence demonstrating a relationship between exemplarity, moral identity religiosity, spirituality, and prosocial behaviors (Blasi, 1980, 1983; Hardy & Carlo, 2005b; Hardy et al., 2012; Walker & Pitts, 1998; Walker & Frimer, 2008). Colby and Damon (1992) were one of the first to suggest that religion and spirituality play a fundamental role in exemplars lives. Of the 23 exemplars that Colby and Damon interviewed, all 23 identified themselves as being associated with some religious affiliation. Among the 23 exemplars, some discussed their faith in a religious God, and some in terms of a spiritual God. Furthermore, most of the exemplars credited their fundamental commitments to values as an association to their faiths. In another study, Walker (1999) sought to compare the Big-Five traits against the personality descriptors of religious and spiritual exemplars. Walker's analysis determined that religious exemplars displayed all of the Big-Five traits. However, in every case as compared to the religious exemplar, the spiritual exemplar displayed significantly higher levels of each of the five personality traits. Because of the apparent association between exemplarity, religiosity, and spirituality, it is a logical endeavor to determine if non-exemplar computing practitioners who identify as being religious or spiritual are less willing to commit privacy violations to PII, than those practitioners that do not have this identification. However, Walker and Frimer caution that the relationships between religion, spirituality, faith and exemplarity are likely complex and interwoven with possibly other constructs.

Blasi (1980, 1983) elucidated the importance of integrating morality into a self-system, as key component of moral exemplars identity formation. Maclean, Walker, and Matsuba (2004) following Blasi's lead, investigated how identity integration and religious orientation interact with moral functioning. Their research sought to determine what interactions if any there were between identity integration, religious orientation, moral reasoning, and self-reported altruism, which are also known as prosocial behaviors. Results indicated that moral reasoning positively correlated with identity integration and an intrinsic religious orientation. The concept of an intrinsic religious orientation as originally described by Allport and Ross (1967), maintains that individuals with an intrinsic religious orientation genuinely believe the doctrines of their religion, so they make every effort to live their lives around those religious beliefs. However, Allport and Ross maintain that an extrinsic religious orientation is where individual's use religion as a means because it serves some purpose. Other results by Maclean et al. indicated that moral reasoning, identity integration and an intrinsic religious orientation accounted for "self-reported altruism" (p. 433), which is the practice of caring for other through prosocial behaviors. Based on the Maclean et al. data, evidence appears to suggest that an intrinsic religious orientation correlates with identity integration, thus suggesting that a link between moral reasoning, religious orientation, and prosocial behavior.

Research has demonstrated that moral reasoning leads to moral functioning, and that without integrating morality into a self-system, a moral identity formation is not complete for the exemplar. Additionally, exemplars moral reasoning, functioning, and identity link with how religiosity manifests in them and that it is partially through their sense of religiosity that their prosocial behaviors egress. However, to what extent and how strong these relationships of religiosity and prosocial behaviors are to identity

formation and reasoning for moral exemplars has not yet conclusively been determined. Therefore, this research asked the following question: Are non-exemplar computing practitioners who identify as religious or spiritual, less willing to commit privacy violations to PII if they also exhibit patterns of high prosocial behaviors, than those practitioners that do not?

Literature that is statistically grounded, or supported with strong theoretical or anecdotal evidence ties exemplarity, moral maturity, and various socio-economic variables to the DITs. As previously discussed, the DITs were designed to activate an individual's moral schemas, and measure one's level of moral reasoning and level of moral maturity (Rest, Thoma, & Edwards, 1997; Rest, Thoma, Narvaez, & Bebeau, 1997; Rest, Narvaez, Thoma, & Bebeau, 1999). According to Rest (1999), the third and highest form of moral reasoning is postconventional thinking. Narvaez (2010) explains postconventional thinking as being able to "step away" (p. 167) from personal interests and coordinate one's thinking and activities towards sharable ideals, such as societal laws. In this manner, postconventional thinking represents more mature moral functioning over preconventional thinking, which focuses more on personal interests.

As one ages, moral reasoning and decision-making become more mature, as is noted by higher p-scores on the DITs (Mujataba, Cavico, McCartney, & DiPaolo, 2009; Rest et., 1999; Rest, Thoma, Narvaez, & Bebeau, 1997). Higher p-scores are also indicators of advanced principled reasoning, or postconventional reasoning. Exemplars exhibit high levels of moral functioning, and thus are likely to present with high p-scores (Narvaez, 2005), though currently no empirical literature substantiates this association. Furthermore, higher DIT scores correlate with age, and level of education (Bebeau & Monson, 2008; Freeman, 2007; Mobley, 2002; Rest, Davison, & Robbins, 1978; Rest,

Narvaez, Bebeau, & Thoma, 1999; Thoma, 2006). That is to say, older more mature individuals, sometimes with more advanced levels of education, especially in professional careers where ethics are a concern (Bebeau, 2002b; Huff & Rogerson, 2005), are also likely to present with higher mature moral reasoning scores. The rationale for this is that, principled moral reasoning and identity, like that of exemplars, generally promote ethical integrity, (Miller & Schlenker, 2011; Narvaez & Lapsley, 2009a), particularly in business environments (Trevino, 1986; Trevino & Brown, 2004). Additionally, Cannon (2001) demonstrated that those individuals with more years of work experience showed slightly higher p-scores; however, only limited literature documents this type of relationship (Mujataba, et al.). One explanation for this ambit of literature documenting moral reasoning and work experience is that much DIT literature revolves around college-based samples. Additionally, it stands to reason, if only anecdotally, that salary might track with higher p-scores of domain specialist exemplars, because the type of domain specialty referred to in this dissertation requires higher levels of education, higher levels of principled moral reasoning and a high standard of integrity. These are factors often associated with domain specialists in fields such as computer engineers, high-level computer programming, university IS/IT/CS professors, and corporate IS/IT privacy officers. As these types of individuals progress in their career they age, and with age generally come higher salaries. Conversely, the power of a higher salary is likely capable of promoting more principled ethical reasoning and decision-making, especially in light of losing one's job over unethical behavior. Therefore, anecdotally, age, education, exemplarity in terms of principled moral reasoning and integrity, may also relate to an overall higher salaries for older, more experienced and better educated IS/IT practitioners. However, while no known literature directly supports

this view, there is more than circumstantial literature to draw this conclusion. Therefore, this research will investigate the association between age, education, salary, and years worked, to determine if as these factors increase, they are related to IS/IT practitioners' lack of willingness to commit privacy violations to PII. Secondly, this research asks if non-exemplar computing practitioners that advance their education beyond a bachelor's degree, are they less willing to commit privacy violations to PII?

*Professional identity.* Exemplar's professional identity varies in accordance with their career domain, and the domains requisite virtue skills and knowledge. For example, the virtue skills and knowledge displayed by an exemplary doctor or attorney are somewhat different from the exemplary virtue skills and knowledge of a computing exemplar. However, within the spectrum of exemplarity, there are those professional exemplar features that appear to transcend the specificity of particular professions. For instance, exemplar professionalism embodies an internalized moral sense of obligation to one's profession, excellence in technical skills, and the importance of self-reflection, along with compassion, honesty and trustworthiness, and a sense of social responsibility directed towards society at large (Hamilton & Monson, 2012). These embodiments not only tie to exemplar professionalism, but also represent fundamental moral structures of the exemplar as a person, because they have become embedded core elements of the exemplar. Therefore, exemplars' professional identity is also a manifestation of their personal identity Colby and Sullivan (2008).

Bebeau (2008) and Bebeau and Monson (2008) provide further support of professional identity formation, citing that dental exemplars are capable of articulating key profession expectations within their career domain. This is similar to computing

exemplars that are familiar with the ACM and IEEE codes of ethics. Because of this, they are capable of maintaining their behaviors based on these organizational codes. Professionalism and code adherence is often important because codes give professional guidance (Stahl & Wood, 2007). Additionally, Bebeau and Monson maintain that exemplars in the professions are aware of their need for lifelong learning and self-regulation. Therefore, it is reasonable to ask the following question: If non-exemplar computing practitioners are aware of organizational or associations' codes of ethics are they less willing to commit privacy violations to PII than those practitioners that are not aware of the code?

Additionally, exemplar professionalism is rooted in purposeful and deliberative actions. Therefore, professionalism in action represents exemplars four influential areas and schemas, and their non-schema dispositional attributes that manifest through virtue skills and knowledge. Hence, computing professionalisms entail causal responsibility, role responsibility, legal responsibility, and moral responsibility. These attributes are articulated by Fuller et al. (2009) in Appendix G, and represent an extension of work presented by Little et al. (1999) on the professional values in computing. Additionally, Appendix H identifies many of the exemplary computing attributes addressed by Huff et al. (2008a, 2008b). Therefore, given the components of moral actions in computing (Appendix H), and the Fuller et al. professionalisms in computing (Appendix G), it is reasonable to believe that computing exemplars display a high degree of responsibility, and that they are willing to take initiatives.



## **Computing Exemplars**

Relative to other career domain exemplar literature (Plaisance, 2011; Rule & Bebeau, 2005; Smith & Godfrey, 2002), Huff and Rogerson (2005) were the first to examine and understand what separated computing exemplars from other types of exemplars. They did this by coding the live narrative stories of 24 computing exemplars. Similarly, Huff et al. (2008a, 2008b) were the first to develop an integrated multidimensional four-component model that explained computing exemplars sustained moral actions using virtue ethics; they labeled the model PRIMES. The purpose of PRIMES was to develop a positive professional pedagogy for teaching computer ethics. The model is grounded in the frameworks of personality, the integration of morality into a self-system, moral ecologies, and virtue skills and knowledge.

From their original coding of the 24 computing exemplars, Huff and Rogerson (2005) were able to discern two types of computing exemplars: craftspersons and reformers. Craftspersons generally focus on client needs in order to articulate and define the goals of their work, thus they often see themselves as service providers of technology artifacts, and “view difficulties or disagreements as problems to be solved” (Huff & Barnard, 2009, p. 50). Craftspersons also believe that their work is towards an ethical end, and in general had a more positive “emotional tone” (Huff & Rogerson, p. 4) regarding their work than did reformers. Reformers had tendencies towards viewing individuals as victims of injustice, such that computer systems lack a public good that they wanted to bring to it. Reformers also viewed barriers as a form of resistance by those that had other interests. Huff and Rogerson also observed that reformers took the role of “moral crusader to reform the system” (p. 5). Reformers had a more negative emotive tone due to the difficulties that linked with systems reform, and because they

recognized that, they held the minority view. Consistent with previous exemplar literature, Huff and Rogerson also found that their computing exemplars “were embedded in, and committed to, social networks” (p. 5) that consciously cultivated and supported their moral causes. In many instances, this support began early in the exemplars career in the form of mentors. Therefore, it is important to determine if non-exemplar IS/IT practitioners who received this type of support are less willing to commit privacy violations to PII.

Further findings suggest that craftspersons might be unique among exemplars because many of the values that they hold are intrinsic to the computing field and “deeply intertwined and dependent upon their technical expertise” (Huff & Rogerson, 2005, p. 5). For instance, quality of service has a distinct meaning in the field of software development; the same holds true for human computer interaction, which refers to how end-users of systems interface with technology. Dissemination of data or access to data is another such intrinsic value, especially where the privacy to PII is concerned. Additionally, Huff and Rogerson remark that some of their exemplars exhibited aspects of both craftspersons and reformers, but that there were more pure craftspersons than there were reformers. Due to this fact, Huff (2011) notes that it is likely that there is no unitary profile of an exemplar to describe how they go about work, this is consistent with the literatures of Walker and Frimer (2007), and Walker and Henning (2004) who suggest multiple exemplar types.

Another uniqueness of computing exemplars is how they inseparably couple their values with their technical skills (Huff et al., 2008a, 2008b; Huff & Rogerson, 2005). This suggests that craftspersons, which may be designers of privacy artifacts, are likely to consider both the context and content of privacy relative to their respect for privacy.

Further findings also suggest that computing exemplars were aware of environmental factors such as budgetary constraints, and organizational factors that may hinder or prompt their ability to act with virtuous intent. Huff (2011) also draws attention to an important fact concerning his exemplars when he states the following:

From their perspective they were not trying to ‘make ethical decisions,’ but instead, they were designing systems for the handicapped, or designing privacy-enhancing software to change business customer relationships, or supporting women in engineering, or changing the way safety-critical software was designed and evaluated, or supporting openness in software design. (p. 5)

This bears mention for three important reasons. First, the exemplars did not set out in ethical deliberation to solve problems, rather they acted with what Huff calls “purposeful-action” (p.2) as opposed to a “deliberative-decision approach” (p. 2) to decision-making. This implies that the computing exemplars innately worked with automaticity towards their moral obligations for a social cause. Second, Huff notes that ethical deliberation was generally not necessary unless something went off course. This implies that these exemplars had developed the necessary skill sets and knowledge to recognize when ethical deliberation was necessary, which is why it is said that computing moral exemplars can and do act with purposeful moral action. In order to do this it is also necessary for the exemplars to have integrated morality into a personal self-system, and have developed the components of a moral personality. Lastly, Huff notes that the exemplars more often discussed the required social skills needed to navigate moral ecologies, and the technical skills required to understand design issues in order to sustain their purposeful moral actions of care. For the purposes of this dissertation, both of these points are critical. Even if an individual possesses a moral personality, has integrated

morality into a self-system, and is capable of navigating moral ecologies, without skills and knowledge, purposeful moral action in computing is not possible, because virtuous actions require learned skills and knowledge. In fact, Huff states that without skills and knowledge, “The highest praise we might summon for the morally committed incompetent would be “well intentioned” but certainly not “virtuous” (p. 5).

This is not to suggest that personality does not play a role in computing exemplar behavior. According to Huff and Barnard (2009), of the Big Five personality traits, neuroticism was the one trait that computing exemplars scored very low on. This is understandable given that this particular trait is a measure of negative emotional reactivity, and stands in opposition to morally grounded behaviors. Not surprising, Huff and Barnard found that reformers scored high on extroversion, while craftsperson scored high on openness to experiences. This makes sense for two reasons. Extroversion is that type of trait needed to bring around reform, and it is required to be able to influence others. Secondly, openness to experience is required for the computing craftsperson in order for them to be able to take on and understand others positions and problems. While other Big Five traits such as agreeableness and conscientiousness did not stand out as notable characteristics of computing exemplars, this may only be a function of the small sample size, especially because these two traits do support virtuous actions and values (Huff & Barnard). For instance, John, Naumann, and Soto (2008) note that scoring high on conscientiousness holds dimensions of achievement via conformance, which relates to success in work environments, and an ability to delay gratification through impulse control. In addition, John et al. remark that agreeableness loads high among the dimensions of cooperativeness, and being trusting and helpful, while John and Srivastava (1999) note that agreeableness correlates with the value of benevolence and a willingness

to donate to charities, both of which are notable prosocial behaviors. Therefore, it makes sense to determine if IS/IT practitioners that donate time and money to charities via their prosocial orientations are less willing to commit privacy violations to PII due to their dimensions of care towards society. Again, because of Huff and Rogerson's (2005) small sample size, it is difficult to reach concrete conclusions regarding all personality traits of computing exemplars, however, Huff (2011) keenly points out that among computing exemplars, personality appears to act as an anchoring point for "moral inclination" (p. 20).

All moral exemplars integrate morality into a self-system. Schlenker et al. (2009) suggested a connection between the self and the moral obligations that exemplars feel, such that morality becomes a commitment of internalized convictions that guide a lifetime of personal and professional behaviors. Huff (2011) noted that his computing exemplars displayed moral commitment as "strategic goals that guide action over time" (p. 4). This notion of strategic guided action is reasonable, given that Huff and Rogerson (2005) recognized the special way in which computing exemplars integrated morality into a self-system, partly by melding acquired skills and knowledge so that their moral self-system became a representation of their moral skills and knowledge. So pivotal was this melding within computing exemplars that Huff and Rogerson proposed a four-component model of computing exemplarity (Appendix H) similar to the four-component model of Rest and Narvaez (1994), and Narvaez, and Lapsley (2005). However, unlike Rest's generalized four-component model that stems from his stages of moral development, and the Narvaez and Lapsley generalized four-component model of moral experts skill-sets, Huff and Rogerson's four-component model specifically addresses the moral expert skills and knowledge of computing exemplars. The first component of the

model is based upon moral imagination, which is the ability to project oneself into the perspective of others. The second component, moral creativity, allows computing exemplars to generate solutions to moral challenges while responding to various constraints. Reasonableness, the third, component is the ability to engage in responding dialog with openness. The last component represents perseverance, which allows for the planning of moral action, and the responding to unforeseen circumstances while keeping moral goals intact. While general overlap is clearly noticeable between the three models for items like sensitivity to societal needs, various moral values, and a sense cultivated respect and judgment, overall it is Huff and Rogerson's components that are aimed directly at the skill-sets and knowledge that are required for a computing exemplar. For instance, this means that these individuals hold in high regard the responsibilities that they have towards society, and that these responsibilities have become internalized such that they have become a feature of the computing exemplars moral self-system. It comes with no irony that Huff and Rogerson specifically mention safety and privacy as key knowledge domains under each of the four components given societal expectations about the safety and privacy of their PII (Nissenbaum, 2004, 2010).

It is at this point that we need to ask if we can expect computing exemplars to respect the privacy of PII for members of society. A possible answer to this question is yes, based on the following facts. Personality traits such as care, respect, and conscientiousness are associated with exemplars (Walker, 1999). Thus, one should expect to see computing exemplars care about and respect the privacy to PII in a conscientiousness manner. Exemplars integration of morality into a self-system means that computing exemplars are likely to have internalized and intertwined ethical conceptualizations of care and respect for PII privacy (Huff et al. 2008a, 2008b), such

that it these concepts have become a part of who they are. Additionally, this integration of morality works in conjunction with computing exemplars moral ecologies such that these environments will either support or thwart their professional moral skills and knowledge (Huff et al., 2008b). When computing exemplars moral skills and knowledge are supported, concepts such as the care and respect for the privacy to PII is realized through ICs and RSOs that come through in their moral decision-making and behaviors to protect PII. Further contributing factors that are also likely to support the computing exemplars decision to protect the privacy to PII are their altruistic natures (Jeffries et al., 2006; Mastain, 2007), and prosocial behaviors (Dunlop, Walker, & Matsuba, 2012; Frimer et al. 2011).

### **Summary**

This chapter has presented empirically grounded and anecdotal evidence supporting the existence of the multidimensionality of the computing exemplar. This review has indicated that a multidimensional view of moral exemplars and computing exemplars is necessary in order to comprehend their varied personalogical dispositions and Hallmark Features. To do this, literature presented a delineation of how virtue and character relate to personhood. Additional research presented indicated that an understanding of the moral-self, moral ecologies and moral skills and knowledge are also necessary in order to build a picture of what moral exemplars and computing exemplars are. Further literature also indicated that other dispositional, and Hallmark Feature non-schema based attributes are likely to influence exemplars decision-making and behavior.

By developing this moral multidimensional view of exemplars, this literature review constructed a framework for understanding, what Hallmark Features likely

contribute to computing exemplars lack of willingness to commit privacy violations to PII. With these understandings, it is now possible to compare non-exemplar computing practitioner's behaviors towards PII privacy, because even though this research does not have a computing exemplar group of comparison, exemplar areas of influence, schemas, and attributes are considered stable enough for comparison. Additionally, with these understandings, a PII privacy violations instrument can be created in order to assess the following hypothesis. Those IS/IT practitioners who identify themselves as possessing some of the predictive Hallmark Features that moral and computing exemplars have, are less likely to commit privacy violations to PII, than those IS/IT that do not identify as possessing some of the Hallmark Features of moral and computing exemplars.



## Chapter 3

### Research Methodology

#### Introduction

The purpose of this chapter is to present in detail the research methods used in this study. The goal of this study was three-fold. The first goal was to develop a reliable and valid survey instrument capable of measuring the severity of PII privacy. The second goal of this study was to determine which non-exemplar IS/IT practitioners were less willing to commit privacy violations to PII, along with what Hallmark Features contributed to practitioners being less willing to commit unethical computing behaviors. Ancillary to the first two goals was to theoretically analyze the results of IS/IT practitioners privacy-based behaviors, and to compare them to computing exemplars, who are known for their virtuous computing practices, and not likely under normal circumstances to commit privacy violations to PII (Huff et al., 2008a, 2008b).

To conduct this study, two phases were required. Presented here is a high-level overview as part of the introduction, with a detailed accounting later in this chapter. In the first phase of this research a set of 40 PII privacy violation questions to PII were developed, and then Subject Matter Experts (SME) assessed the severity of these privacy violations in order to construct a privacy violations questionnaire and scale that was administered to IS/IT practitioners. This initial SME survey is known as the Privacy Pre-Survey Scale (PPSS). The second phase of this study entailed developing the actual IS/IT practitioners PII Privacy Violations Scale (PPVS) from the PPSS, and adding a moral exemplar identity Hallmark Features section to it. From this, the PPVS was administered

to IS/IT practitioners to determine which practitioners were less willing to commit privacy violations to PII.

Johnson and Onwuegbuzie (2004) concluded that the greatest opportunity for meaningful results in research is to have a study's methodology follow its research questions. In the purest sense, the approach used in this study is quantitative, because it relied on experimental procedures, surveys, and data collection in order to conduct statistical analysis (Creswell, 2011). However, given that, no discernable literature presently existed at the time of this research with regards to IS/IT practitioners' privacy violation behaviors, this research was also descriptive and theoretically exploratory in nature.

## **Methods**

**Phase one development.** The PPSS (Appendix I) consisted of SMEs demographic questions, and 40 questions representing privacy violations to PII that IS/IT practitioners could commit. These questions are theoretically grounded on the Intermediate Conceptualizations of IS/IT PII privacy, and are intended to portray the opposite of what IS/IT practitioners Role Specific Obligations (RSOs) to PII should be. This is to say, that the appropriate RSO towards the privacy of PII should be its protection, and not its violation. Theoretically, these questions also represent behaviors that computing exemplars are not likely to commit under general circumstances due to the manners in which they have integrated morality into their lives and careers, their moral knowledge and skill sets, their personality, and their moral ecologies. These questions were developed from the author's expert knowledge of privacy violations to PII. Given the theoretical nature of this research, and that no computing exemplar

population was available as a comparison group, assessment of morally correct behaviors towards PII privacy requires some form of grounded validation. Davis (1992) and Nunnally and Bernstein (1978) suggest that expert panels should appraise instruments developed from theoretical or conceptual frameworks to assess the accuracy of content questions. Therefore, a group of SMEs assessed the severity of these 40 unethical IS/IT PII privacy violations to PII using the following seven-point forced-choice Likert type scale where: 0 = No Violation, 1 to 2 = a Minimally Unethical violation, 3 to 4 = a Moderately Unethical violation, and 5 to 6 = a Highly Unethical violation. The deviations between the scales numbers were used for refining the interpretive values of how unethical a particular privacy violation scenario was. That is to say; the ordinal scale used for this research allowed SMEs to express the relative magnitude or severity for each of the 40 privacy violation questions.

***SME population.*** The criterion used for SME inclusion in this study was as follows. Each SME had a minimum of 10 years career experience dealing with technologies, privacy, and PII, and come from the fields of academia or industry. The 10-year criterion assumed exposure to a wide range of privacy-based issues that fewer years may not capture. Additionally, this criterion was consistent with Bebeau and Thoma (1999), and Keefer and Ashley (2001) who indicated that moral-reasoning and decision-making capabilities increase with years of experience. Deemer (as cited in Rest, Thoma, Narvaez, & Bebeau, 1997) further supports that 10 years appears to be the demarcation of life experience that influences moral judgment in adults. Therefore, it is believed that 10-years of career experience would be long enough for the SMEs to have become well enough entrenched in their careers to recognize IS/IT privacy violations to PII. This 10-

year mark also assumed a certain level of understanding for what an ethical and unethical behavior is. In addition, the aim was to collect data from between 30 and 40 SMEs within a 30-day cut-off period. The actual number of SME participants came to 53. These high numbers are justified for the following reasons. Privacy is multidimensional and is represented by many multidisciplinary fields that are at least comprised of computer ethicists, IS/IT professors, public policy specialists and professors, law experts in and outside of the field of academia, chief privacy officers within organizations, and security and privacy experts or specialist that are consultants to government and industry. Therefore, one would want SMEs from multiple career domains.

The 40 PII privacy violation questions developed for this research took the following leads from previous literature. Based on Dillman (2000), one should avoid grammatical complexities, thus questions used active instead of a passive voice, and avoided over use of pronouns to reduce cognitive demands from survey participants. Further reduction in cognitive load was obtained by avoiding words that conveyed degrees of vagueness (Dillman). Therefore, words such as, or similar to, perhaps, maybe, frequently, usually, regularly, I think so, were purposefully not included in the PPSS. Lastly, Foddy (as cited in Lietz, 2008) recommends five-point Likert scales for questions, “requiring absolute judgments” (p. 11), and seven- to nine-point Likert scales when abstract assessments are required. Given that the PPSS requires absolute reasoning, that is to say reasoning for assessment of abstract interpretations to the intermediate conceptualizations of PII privacy violations, a median seven-point Likert scale was selected for the SMEs to work with.

**Data collection.** Increasingly the Internet has become a prominent environment to administer Web-based surveys (Baatard, 2012; Van Selm & Jankowski, 2006). In comparison to the development and deployment of a Web-based survey, a mix-method deployment of paper-based, email-based, and Internet-based surveys is more time-consuming and costly (Greenlaw & Brown-Welty, 2009). Additionally, when compared individually to Web-based survey development and deployment, paper-based surveys are also not as response effective as are Web-based surveys (Greenlaw & Brown-Welty). Furthermore, Web-based surveys also provide the following: online database repositories for survey participant's responses, instant data retrieval, they generally allow for larger sample sizes, allow data importation into any number of database, spreadsheet, and statistic packages for analysis, and permit participation at a convenient time for the research subject (Bennett & Chenicheri, 2010; Evans & Mathur, 2005). Therefore, development and deployment of the PPSS was conducted via the Internet using the Web-based survey service of Surveygizmo.com. Once the PPSS data was retrieved a rank ordering of the top five items in each of the three categories of minimally unethical, moderately unethical, and highly unethical privacy violations to PII were extracted from the data sets.

Prior to data collection, SMEs were contacted via LinkedIn. After accepting the Connect Invitation in LinkedIn, an email invitation via LinkedIn was sent to the SMEs requesting their participation with the PPSS, this invitation also included a link to the survey at SurveyGizmo.com (Appendix J). Upon logging on to SurveyGizmo.com to complete the PPSS the SMEs were presented with an introduction explaining the survey (Appendix K), and then detailed instructions for how to complete the survey (Appendix L). In addition, the instructions on the Surveygizmo.com Website reminded the SMEs

that participation in the survey was completely anonymous, that is to say their responses would in no way be associated to their names in this research. As a further precaution to protect anonymity, IP address tracking was shut-off in SurveyGizmo.

*Data analysis.*

*Descriptive statistics.* The SMEs descriptive demographics are presented in Appendix M. The measures of central tendency, and the measures of central tendency along with each Cronbach alpha if each particular privacy question was deleted from the 40 privacy violation questions are presented in Appendix N and O, respectively. Appendix P displays all 40 privacy violation questions based on their descending mean values. Lastly, Appendix Q presents the SMEs response frequencies to all 40 of the privacy violation questions. The information contained in these appendices were used to ensure that there were no outliers that would skew the data, and to determine the first five minimal, moderate, and highly unethical privacy violations to PII. Further discussions of these descriptive measures are presented in the results chapter of this dissertation.

*Reliability.* Internal consistency explains the extent to which all of the items in a test measure inter-relate; it is an “evaluation of measurement accuracy” (Straub, 1989, p. 151). One of the most often used measures of test-score reliability from a single test administration is Cronbach’s Alpha coefficient (Webb, Shavelson, & Haertel, 2006), hereafter known as alpha. Alpha is also a measure of internal consistency for continuous item responses on Likert type scales (Helms, Henze, Sass, & Mifsud, 2006), and “indicates how well the items in a set are positively correlated to one another” (Sekeran, 2003, p. 307). Sekeran further states that alpha can take a range of zero to one, with a one indicating a positive correlation coefficient between all test items. Tavakol and

Dennick (2011) remarked that acceptable levels of alpha are between .70 to .95. Similarly, George and Mallery (2003) provide the following rules with regards to alpha: “ $\alpha > .9$  – Excellent,  $\alpha > .8$  – Good,  $\alpha > .7$  – Acceptable,  $\alpha > .6$  – Questionable,  $\alpha > .5$  – Poor, and  $\alpha < .5$  – Unacceptable” (p. 231). However, when high inter-correlations are attained, cautious interpretation is warranted because it might mean that test items are overly redundant (Briggs & Cheek, 1986). The Cronbach’s alpha for the PPSS was a .93.

*Validity.* It is not enough for a survey instrument to be reliable; it must also prove to be valid in order to generalize its results. Validity is the extent that an instrument measures what it purports to measure (Tavakol & Dennick, 2011). Expert panels help to establish the content validity of an instrument with their qualitative assessments (Davis, 1992; Wynd, Schmidt & Schaefer, 2003). Establishing content validity for a new metric is vital because it links abstract conceptualizations to observable and measurable instances of instantiations that the researcher is looking for. Additionally, content validity can aid in establishing construct validity, which gives confidence to readers and researchers about a new survey instrument (Yagmaie, 2003). In the case of the PPSS, the SMEs established validity with their subjective ratings and rankings, as is reported in Chapter Four.

**Phase two development.** Originally, the proposed research of this dissertation was to run one PPVS, in order to determine which IS/IT practitioners would be more and less willing to commit privacy violations to PII based upon a number of different predictors. However, an initial visual inspection of the data from the PPVS indicated that privacy violations were being committed. Therefore, two follow up surveys were also

developed. These other two PPVSs asked different privacy violation questions. The three PPVSs are distinguished from one another in this research by their respective labels of PPVS-1, PPVS-2, and PPVS-3. A complete explanation of these three surveys follows throughout this chapter and the following results chapter.

Each of the three PPVSs contained two sections. The first section of each PPVS comprised the five sections of the Hallmark Features section (Appendix R). The five-Hallmark Features sections presented in this research are, Career-Organizational Values, Religion and Spirituality, Ethics-Training-Awareness, Prosocial Behaviors, and General Demographics. Each of the five sections included multiple questions designed to, at least in theory, tap moral and computing exemplar Hallmark characteristics. The second section of the PPVSs contained 15 privacy violation questions to PII. For each of the three PPVSs IS/IT practitioners had one of five responses that they could select from, that would determine the likelihood of committing the privacy violations. These responses were as follows: 1 = I would always do this; 2 = I would probably do this depending on the circumstance(s); 3 = I am not sure what I would do; 4 = I would probably not do this depending on the circumstance(s); and 5 = I would never do this. PPVS-1 (Appendix S) contains the five most minimally, the five most moderately, and five most highly unethical privacy violations to PII that were evaluated and ranked by the SMEs on the PPSS. Further refinement of these 15 items was also based on the least amount of variance found in the questions, and is reported in the following analysis chapter. The PPVS-2 (Appendix T) contains the 15 most minimally rated and ranked of all 40 privacy violations to PII, and each privacy violation ended with the same question to the practitioner's that the PPVS-1 did, which is "What would you do? Please select one response from below." The PPVS-3 (Appendix U) contains the same 15 privacy



violation questions to PII that the PPVS-2 did, except the ending of the questions differed in that it asked; “If no one could ever find out that you did this, what would you do? Please select one response from below.” The limitation of 15 PII privacy violation questions to PII was based on the work of Burchell and Marsh (1992), and Porter (2004), who have substantiated that shorter questioned surveys have higher and more accurate response rates. Therefore, IS/IT practitioners respond to these 15 questions by indicating their willingness, or thereby lack of willingness to commit these privacy violations to PII with the non-forced-choice five-point Likert rating scale.

Much literature has discussed the number of scale points for surveys (Chafouleas, Christ, & Tiley-Tillman, 2009; Cox, 1980; Friedman, Wilamowsky, & Friedman, 1981; Garland, 1991; Komorita 1963; Lietz, 1980, Matell & Jacoby, 1971; Preston & Colman, 2000; Wildt & Mazis, 1978), with no absolute consensus for how many Likert points are best, although general agreement suggests no less than a five-point scale. However, Courtenay and Weidmann (1985) and Adelson and McCoach (2010) concluded that scales that include a mid-point tend to enhance reliability, while Kalton, Roberts and Holt (2009) suggest that survey participants that are offered a mid-point more often select this option. Clearly, differences of opinion in the literatures do exist. However, Tsang (2012) remarks that researchers should only use a mid-point on a Likert scale, if the researcher clearly knows and identifies what the mid-point means. For the privacy violation questions to PII a non-forced mid-point scale was chosen to permit some ambiguity, and additionally, it assumes the possibility of the IS/IT practitioner still committing the PII privacy violation. It is with these understandings that a mid- five-point scale was selected for the PII privacy violation responses.

The dependent variable used in this study was the three variants of the 15 privacy violation questions that comprised each of the PPVSs. The independent variables for this research comprised individual and in some cases, composites of questions from Hallmark Features section, which contained five sections and 53 questions (Appendix R). The nine predictors used to help determine the validity of the hypothesis were as follows. The composite score for religiosity and spirituality, and the composite score for prosocial behaviors. Additionally, questions seven and eight from the first section of the Hallmark Features section were selected because they helped identify if an individual considered themselves ethical; this too was a composite question. Lastly, age, level of education, household income, years worked in the IS/IT field were also selected, and whether a practitioner had ever had any type of ethics training, along with whether or not someone said that had had a career moral mentor.

As previously discussed in the Literature Review's Summary, the selection of the independent variables was based on the following. Recently, Johnson (2012) reported that previous literatures have demonstrated significant associations between exemplars, organizational values and types of career, and that organizational values associate with religion and spirituality, ethical awareness and ethical decision-making, and prosocial behaviors. Similarly, Maclean et al. (2004) reported significant findings between exemplars, ethical reasoning, religion, and spirituality, while Walker and Reimer (2006) noted the relationship between moral exemplars, and moral and spiritual development. Further findings by Emerson and Mckinney (2010) demonstrate the strong underpinnings of ethical behaviors and religious values in business. This is of consequence because the sample populations used in this research are working IS/IT practitioners. In like fashion, Carlo et al. (2006) highlights exemplars prosocial behaviors. Given that exemplars

display ethical and prosocial behaviors, it theoretically makes sense that ethical awareness and prosocial behaviors might be strongly associated. Lastly, Einolf (2013) demonstrated that spirituality and religion are statistically related to prosocial behaviors. Clearly, evidence points to statistically significant relationships between exemplarity, religion and spirituality, ethics, and prosocial behaviors. Combined, the first and second parts of the PPVSs will attempt to answer the following question: Are those IS/IT practitioners that identify themselves with the Hallmark Features of moral and computing exemplars less willing to commit privacy violations to PII than are those practitioners that do not identify themselves with the Hallmark Features of moral and computing exemplars.

*Population sample.* This research used three anonymous IS/IT practitioner populations. Because the populations were, specifically working IS/IT practitioners, the samples were purposeful. These populations also represented a convenience sample, because they come from the purposeful pool, and had the option to participate in this survey-based research. The PPVS-1 and PPVS-3 populations were comprised of working IS/IT practitioners that were solicited from LinkedIn. The PPVS-2 population sample was obtained using Cint USA, Inc., a global market research company that supplies survey participants for research based on criteria set by researchers. To ensure no duplicate participation between the PPVS-1, PPVS-2 and PPVS-3, the last question on the PPVS-2 and PPVS-3 asked, “Have you within the past 30 days taken another survey that resembles this one?” The criterion used for inclusion in all three survey samples, was that the IS/IT practitioners be employed fulltime. For the PPVS-1 and PPVS-3, an invitation email (Appendix V) to participate in the survey was sent to LinkedIn members

who accepted this researcher's initial connection invite. In some instances CIOs, CISOs, or CPOs from LinkedIn assisted in distributing an email (Appendix W) to their colleagues and coworkers in order to help obtain survey participants for the PPVS-1 and PPVS-3.

Because many sub-domains exist in the IS/IT fields, extensive efforts were made to obtain the greatest depth and breadth in sampling. To this end, three approaches were employed with the PPVS-1 and PPVS-3 LinkedIn members. The first method employed searching for survey participants in LinkedIn by Technology-based Job Titles (Appendix X). The second method used the Technology-based Job Titles also, but included a search for participants by country (Appendix Y). The last approach entailed obtaining survey participants by corporation names (Appendix Z), which included both national and international corporations.

***Data collection.*** Prior to the actual implementation of the PPVSs, 10 pilot case studies were conducted to flush out any problem questions, and to determine that average time to complete the PPVS survey. The mean time test participants took to complete the survey was thirty-five minutes and twenty-five seconds. As previously discussed, the Internet has become a prominent medium in which to administer surveys for research (Baatar, 2012; Van Selm & Jankowski, 2006). As Bennett and Nair (2010) and Evans and Mathur (2005) have indicated; Web-based surveys offer the ability of database repositories, which allows for instant data retrieval. Additionally, online Web-based survey services enable researchers to export data into a number of statistics packages, and spreadsheet, as well as reducing human data entry errors (Flemming & Bowden, 2009). Therefore, the development, deployment, and retrieval of the PPVSs were conducted

using the Web survey-based services of SurveyGizmo.com. The PPVS-2 was also run this way with a porting function directly to the Cint participants. However, prior to the actual deployment of the PPVSs, 10 test cases were run through SurveyGizmo to ensure that the surveys functioned correctly.

When a participant first logged into the survey at SurveyGizmo, a participation introduction to the study was displayed (Appendix AA). This introduction described that the survey was part of a Ph.D. candidate's research, it explained the purpose of the research, and it assured participants that the survey was completely anonymous. To ensure full anonymity, the IP address capture function in SurveyGizmo was deactivated. In addition, the introduction gave indication to the time that it would take to complete the survey, and that participants could opt-out at any time during the process of filling-out the survey.

***PPVSs data analysis.*** Responses from all three surveys were checked for possible missing data, linearity, outliers, homoscedasticity, and multicollinearity. The purpose of these checks were to ensure that no extreme data affected the accuracy of the analyses results, and so that the possibility of committing a Type I or Type II error was minimized. The results of this data screening and cleaning are reported in the analysis section of this dissertation.

***Descriptive statistics.*** Prior to running inferential analysis, descriptive exploratory analyses were run on all three PPVSs; this information is presented in Chapter Four. The use of the exploratory analyzes was in part used to describe the sample populations

numerically. Additionally, the descriptive analyzes help confirm that information was not distorted by corrupted or inaccurate data.

*Inferential statistics.* To learn about the relationships between the interval-based dependent variable and the multiple predictors from the Hallmark Features sections, multiple linear regressions is the most appropriate approach because it takes into account the covariance among the predictors, and their impact on the dependent variable. Originally, it was proposed that Principle Components Analysis (PCA), Nonlinear Principle Components Analysis (NLPCA) would be run for the purposes of data reduction of the independent variables. However, Budaev (2010) and Osborne and Costello (2004) warn that without large sample sizes, and an adequately large enough item question pool size to draw upon, underfactoring is likely to produce error rates with PCA; this also holds true for NLPCA. As a check, a PCA was run on three of the predictors that had multi-question items as predictors. These were religion and spirituality, prosocial behaviors, and questions seven and eight from the first section of the Hallmark Features. Because only one factor was able to be extracted from each of these predictors, Cronbach alpha's were run on these items to ensure reliability. These results are addressed in the following results chapter.

## **Summary**

This chapter has described the descriptive and exploratory nature of this study's methodology. The methodology included creating a 40 question privacy violations to PII survey that SMEs rated and ranked on a 5-point Likert-based scale. These rankings represented minimally, moderately, and highly unethical privacy violations to PII. From

this SMEs survey, three separate PPVSs were developed that all contained 15 different privacy violation questions. All three surveys contained the same Hallmark Features questions. PPVS-1 contained five minimally, moderately, and highly unethical privacy violations to PII. Both the PPVS-2 and PPVS-3 contained the first fifteen lowest, or minimally invasive privacy violations to PII, however the endings to these violation scenarios differed somewhat. The PPVS-2 ended the privacy violation question by asking participants what they would do based on a five-point Likert scale, while the PPVS-3 ended the privacy violations scenarios in the same mann but also asked participants, “If no one would ever know you commit the violation would you do it?”

One important caveat requires attention with respect to the statistical analyzes that were required to complete this research. Particular consideration was given to sample size. Literatures demonstrate much disparity with regards to sample size and multiple linear regressions. Much of this dissention revolves around the sample size of N being a set number, or a ratio of subject-to-variables (Henson & Roberts, 2006; Preacher & MacCallum (2002). Due to limitations in the final collected sample sizes for each of the PPVSs populations, the questions posed in the Literature Review that were meant to assess the validity of the hypothesis had to be scaled back. Support for this reduction of predictors came from Babyak (2004), Green (1991), Maxwell (2004), and Vittinghoff and McCulloch (2007), who address sample size to predictor ratios. Some literatures suggesting that a sample size of 10 observations per predictor is sufficient, while other literature such as that from Green suggests that in some cases one may need as many as 50 observations per predictor. Since no singularly definitive source can acknowledge what one criterion to use, this research used the mean of 30 observations per predictor, which came from adding and then dividing by two the numbers of 10 and 50. The nine-

predictor variables for this research were the composite score for religiosity and spirituality, and the composite score for prosocial behaviors. Additionally, questions seven and eight from the first section of the Hallmark Features section were selected because they helped identify if an individual considered themselves ethical. Lastly, age, level of education, household income, and years worked in the IS/IT field were also selected, along with whether or not someone said that had had a career moral mentor.



## **Chapter 4**

### **Results**

#### **Overview**

The goal of this research was to conduct an exploratory analysis and determine if those IS/IT practitioners that identify with some of the Hallmark Features of moral and computing exemplars were less likely to commit privacy violations to PII, than were those IS/IT practitioners that did not identify themselves with the Hallmark Features of moral and computing exemplars. This chapter discusses the findings of this research with detailed explanations of the conducted analyzes.

#### **Subject Matter Experts Pre-Privacy Violations Survey**

Prior to collecting and analyzing the data for the PPVS-1, PPVS-2, and PPVS-3, the SMEs PPSS data was collected and analyzed. Data screening revealed no unusual outliers. Of the 153 SMEs invited to participate in the PPSS, 53 SMEs completed the PPSS, for a response rate of 34.64%. The SMEs demographics (Appendix M) describes participant's education levels, occupation, years at occupation, country of origin, and what industry certifications they held at the time of participation. A brief synopsis of the demographic data reveals that doctoral and master's degrees were the norm, while the most frequently occurring occupations were chief privacy officers, IS/IT professors, and privacy specialists. The average years of career experience came to 17.66 years, and the majority of SMEs were from the United States. Overwhelmingly, the most represented industry certification was that of the Certified Information Privacy Professional (CIPP). In addition, the measures of central tendency for each of the 40 privacy violation

questions that were rated and ranked by the SMEs is presented in Appendix N, while Appendix O displays the same information, but in descending order of the mean values.

Prior to developing and deploying the PPVSs, a Cronbach's alpha was run to measure the internal consistency and reliability of the privacy violations to PII that the SMEs rated and ranked. The returned Cronbach was a .93. While different literatures debate acceptable ranges for alpha (Tavakol & Dennick, 2011; Webb, Shavelson, & Haertel, 2007), most literatures accept that alpha's below .70 are not reliable because they indicate a multidimensional association between measures of a construct (Cortina, 1993; Helms, Henze, Sass, & Mifsud, 2006; Kuijpers, van der Ark, & Croon, 2013). Likewise, the closer to 1.0 that an alpha comes, the greater its reliability in measuring a unidimensional construct. Additionally, and based upon the robust multidimensionality of the SMEs, this .93 Cronbach should be considered a very stable measure. Presented in Appendix P are all 40 privacy violation questions with measures of central tendency and their Cronbach's if the privacy scenario were to be deleted. Appendix Q are the serialized SMEs privacy violation questions response frequencies.

### **IS/IT Practitioners PII Privacy Violations Scale (PPVS)**

Originally, the proposed research of this dissertation was to run one PPVS, in order to determine which IS/IT practitioners would be more and less willing to commit privacy violations to PII based upon a number of different predictors. However, an initial visual inspection of the data from the PPVS indicated that some privacy violations were being committed. Therefore, two follow up surveys were also developed. This research made use of three different PPVSs, which were the PPVS-1, PPVS-2, and PPVS-3. The Hallmark Features sections of all three PPVSs were the same except that the last question

on the PPVS-2 and PPVS-3 asked, “Have you within the past 30 days taken another survey that resembles this one?” In no instance did any survey participant say that they had taken a survey similar to the PPVSs within the past 30 days.

Further distinguishing features of the PPVSs were as follows. The first 15 privacy violation questions used on the PPVS-1 were completely different from the 15 privacy violations on the PPVS-2 and PPVS-3. The PPVS-1 used the five most minimally unethical, five most moderately unethical, and five most highly unethical privacy violations to PII that were based on the SMEs ratings and ranking of all privacy violations (Appendix P and Appendix S). This is as opposed to the 15 most minimally unethical privacy violations that were used on the PPVS-2 and PPVS-3 (Appendix P and Appendix S). Both the PPVS-1 and PPVS-2 ended the privacy violation questions in the same manner; participants were asked how likely they were to commit the privacy violation. However, the PPVS-3 ended each privacy violation question in the following manner; “If no one would ever know that, you would commit the violation would you do it.” Testing the willingness to commit privacy violations in the manner was not only a matter of the privacy violation willingness, but also how the questions ended. The purpose for using all three surveys can be explained like this. Since the PPVS-1 made use of the widest spectrum of privacy violation questions and given that practitioners were willing to commit these violations, it made sense to investigate what the practitioners would do with less severe privacy violations. Since the practitioners were willing to commit even less severe privacy violations, it stood to reason that no one would intentionally do something wrong with the perception of getting caught. Therefore, the PPVS-3 asked the same privacy question as the PPVS-2, but with the distinction that the practitioners knew that no one knew that they had committed the

violation. Thus, the PPVS-2 was designed to act as a conduit to the PPVS-3, which presented the most reasonable real-world situation, in that it is highly unlikely that someone would commit a violation with the knowledge that they would get caught.

Throughout the remainder of this PPVS section, analyzes are presented for each PPVS in their own subsections. The one exception to this is the pre-analysis data screening and cleaning, presented immediately below.

**Pre-Analysis Data Screening and Cleaning.** Before data screening and cleaning was performed, two procedures were implemented. A one-time reverse coding procedure was completed in SPSS for survey participants prosocial and age scores in order to get all predictor variables in the correct low-to-high orientation. This reverse coding was based on the coding scheme of survey responses before composite scores were computed. Additionally, a split-file output function based on survey group was implemented prior to running analyzes so that the data that was run, was specific to its own PPVS.

Prior to running any analysis, data normality was verified. Running regression on data requires that certain assumptions not be violated. Therefore, the following checks were performed. Histograms verified normality; examination for linearity was investigated, univariate and multivariate outliers were looked for, assurances were made that there was not multicollinearity, and homoscedasticity was verified to not exist.

Because each variable displayed symmetry against the normal Gaussian distribution, no further investigations for skewness were pursued. A further assumption of multiple regressions is that of linearity. Collectively, examination of each of the predictors showed that there was a linear relationship for each of the generated

scatterplots for the outcome variables. Therefore, no further investigation for curvilinear relationships was performed.

In order to check for univariate outliers, all predictor variables were converted to standardized z-scores. Only two prosocial cases at 3.23 and a single case of age at 3.10 were noted. Ultimately, these three cases were determined not to influence the predictive accuracy of the regressions, so they remained within the datasets. In addition, a Cook's distance and Mahalanobis distance were run to determine if there were any multivariate outliers. Cook's distance measures the influence of single case observations based on total changes in all other residuals when the case is deleted from the estimation process, and is one of the most representative measures of influence for overall fit (Chatterjee & Hadi, 1986; Kim, 1996). A visual check of Cook values was performed to ensure that no value was over one (1). This ensured that no substantial influences were affecting the estimated regression coefficients.

In order to determine leverage points that may unduly influence other predictor variables, Mahalanobis distances were conducted because they consider how far an observation is from the mean values of the predictor variables (DeMaesschalck, Jouan-Rimbaud, & Desire, 2000; Penny, 1996). The critical Mahalanobis value for this research was 23.58 at a 95% confidence level. This critical value was based on a Chi-square of nine degrees of freedom. Inspection of the Mahalanobis data showed six cases that were over the 23.58 value. Two cases were from PPVS-1, and they represented 24.52 and 28.43, one case came from PPVS-2 and it was a 25.31, and lastly three cases were from the PPVS-3, and they were 29.68, 29.85, and 30.32. Because such outliers may present adverse effect on regressions, separate regressions were conducted with and without these

values for their appropriate PPVSs. Given that, none of these cases provided any undue or negative influence on the regressions, they remained in the datasets.

Three scatterplots (Figure 5, Figure 6, and Figure 7) for PPVS-1, PPVS-2 and PPVS-3, were constructed to test for homoscedasticity. Each scatterplot revealed that error variances were constant across the dependent variable criterion.

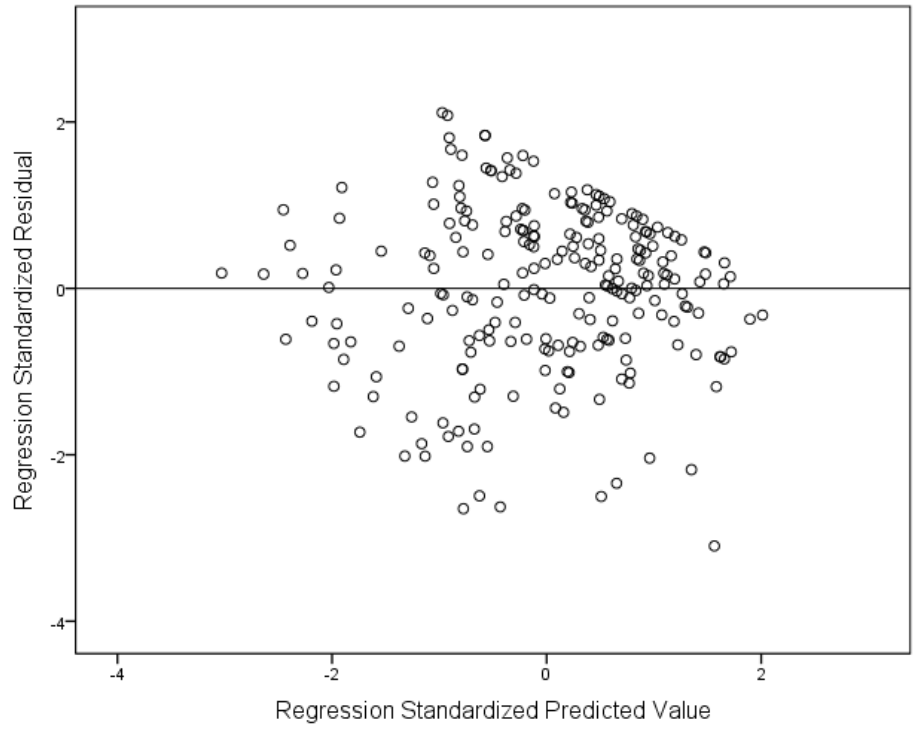
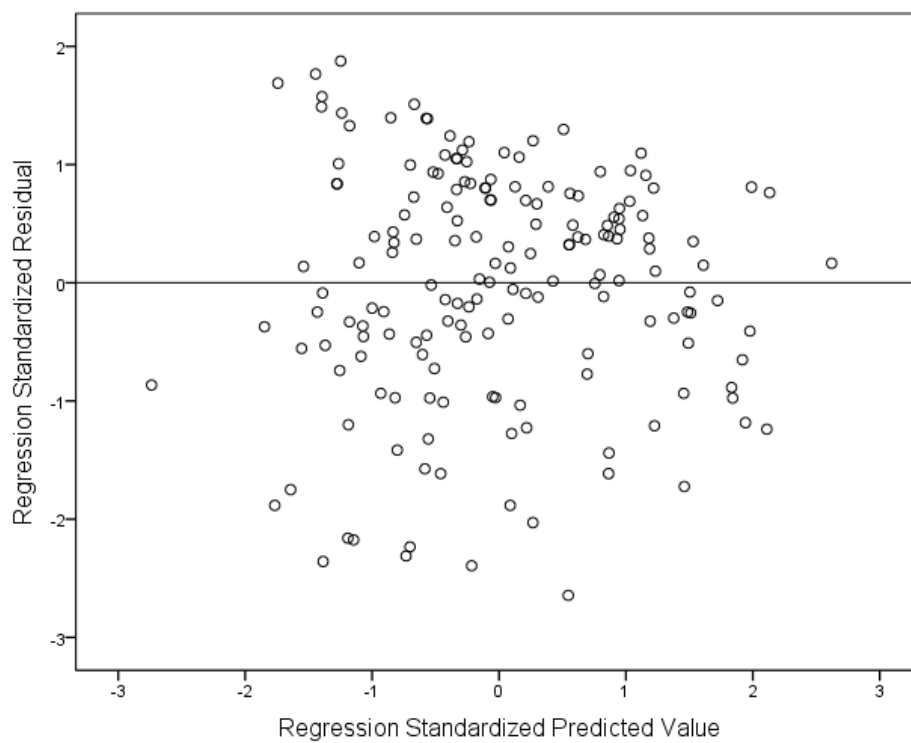
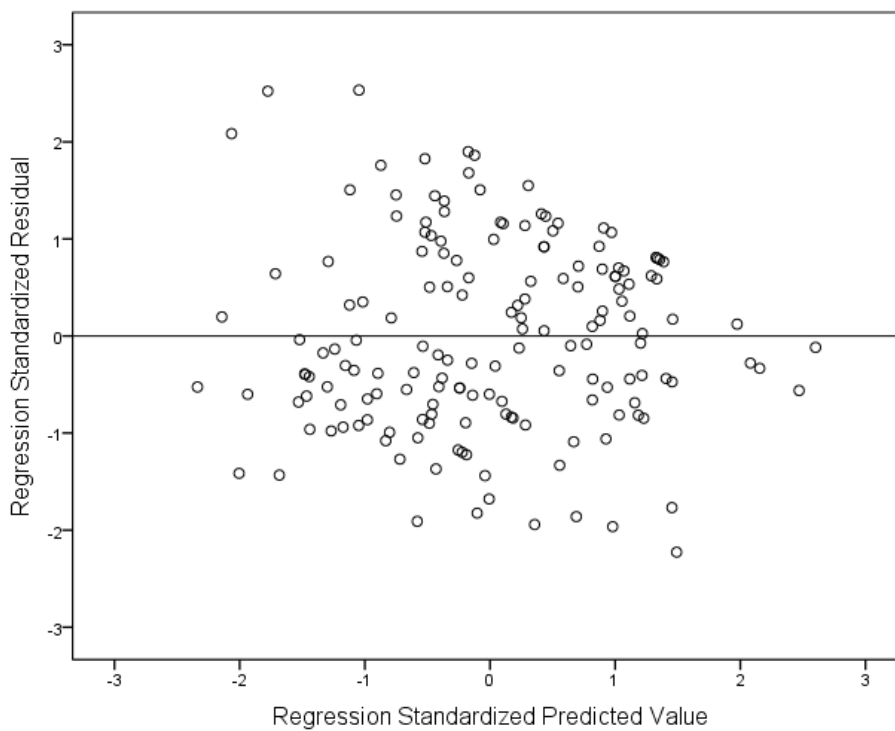


Figure 5. Residual Plot for PPVS-1



*Figure 6.* Residual Plot for PPVS-2



*Figure 7.* Residual Plot for PPVS-3

Lastly, Variance Inflation Factors (VIF) were computed for each of the predictor variables for each of the PPVS regressions. These tests for multicollinearity are reported under each of the individual PPVS sections below, along with the computed regressions.

**PII Privacy Violations Scale-1 (PPVS-1).** As previously mentioned, the PPVS-1 was comprised of the SMEs five most minimally, five most moderately, and five most highly unethical privacy violations to PII, and the Hallmarks Feature section (Appendix M). Even though a Cronbach's Alpha was calculated for all 40 of the SMEs privacy violations to PII, an alpha was also run on the PPVS-1's 15 privacy violation questions to ensure reliability of the intercorrelations among privacy violation questions. The returned alpha was a .87. Based on this alpha, and standard acceptable statistical practices for alpha, this .87 does suggest that the privacy violation questions to PII measured the same construct, and were not redundant.

These 15 violations were selected based upon their relative means, with further refinement for selection based upon smallest variances in most cases. The exception is that question one (Appendix O) should have been selected, and was an oversight, thus question number five (Appendix O) should not have made it into the pool of 15 questions, however it did. Therefore, the questions that comprised that first Cronbach's alpha and that were used for PPVS-1 were as follows: Question 14, 16, 21, 35, 5, 40, 4, 11, 20, 15, 10, 6, 9, and 37.

Presented in Appendix AB are the demographics for the first survey's sample population. The participants for this survey all came from connections on LinkedIn. Briefly, the PPVS-1 consisted of a sample size of 235 participants. Of the subjects, 160 or 68.1% came from the United States. The majority of participants were men; this



represented 90.2% of the sample population. The two age groups most present in the PPVS-1 were the ages of 40-49 and 50-59, which represented 31.5% and 28.9% respectively. In terms of education, a master's degree appeared more than any other degree at 40.4%. One-hundred and eighty or 76.6% of the sample populations identified themselves as married. When asked about children, 32.3% stated they had no children; this was closely followed by 28.5% with two children. The most frequently cite household income was >\$150,000.00 at 26.8%, and 38.7% of the sample populations had 20+ years of IS/IT experience. Following these demographics in Appendix AB are the frequencies of job descriptors or job titles, what industry certifications were held by these individuals, and the IS/IT organizations and associations that they belonged to. Lastly, job descriptors, industry certifications, and organization and association memberships do not total the amount of participants in the sample, because it is common for IS/IT practitioners to hold multiple industry certifications, and belong to multiple industry organizations and associations.

Because the sample size was not large enough, that is to say, there were too few cases per predictor; PCAs were not run on predictors with multiple variable questions. However, Cronbach alphas were run for the three composite indexes of religiosity and spirituality, prosocial behaviors, and questions seven and eight from the first section of the Hallmark Features section that was meant to measure if practitioners thought they were ethical. The Cronbach's for religion and spirituality, prosocial behaviors, and question seven and eight came back as .80, .97, and .70 respectively. The lower reliability for questions seven and eight may be attributed to the fact that only two inter-item variable questions were used to assess how ethical someone thought they were. All other single item predictors were individually added to the regression model.

A multiple regression analysis was conducted to evaluate how well the predictors measured a lack of willingness to commit privacy violations to PII. The nine predictors used in this regression, and the other two PPVSs were: 1) Religion and Spirituality, 2) Prosocial Behaviors, 3) Age, 4) Years Worked in the IS/IT Field, 5) Consider Myself Ethical (Question 7 & 8 – Hallmark Features Section 1), 6) Had a Work Role Model or Mentor 7) Ever Had Ethics Training, 8) Highest Level of Education, and 9) Household Income. The criterion variable was IS/IT practitioner willingness to commit privacy violations to PII. Overall the model was able to significantly predicted when an IS/IT practitioner might be less willing to commit privacy violations to PII at a CI of 95% and an,  $F(9, 232) = 11.87, p = .001, R^2 = .32$ , with an adjusted  $R^2 = .30$ . This indicates that 32% of the model explains why a privacy violation to PII might not take place. Said another way, it explained 32% of the variation in the DV.

The model's descriptive statistics and regression coefficients, along with the VIFs are listed in Tables 2 and 3, respectively. Additionally, the model's correlation tables appear in Appendix AC. As expected, some of the predictors, and coefficients indicated that those IS/IT practitioners that score high on various Hallmark Features were less likely to commit privacy violations to PII. Individuals scoring high on prosocial behaviors and the composite question of seven and eight, that is to say, if a person believes that they are ethical, displayed significance at  $\beta = 0.31, p = .000$  and  $\beta = 0.20, p = .002$ , respectively. This indicates that those individuals that see themselves as prosocial or being ethical were less likely to commit privacy violations to PII. This is an accurate estimate given that all previous assumptions of regression were met, and that the reported VIFs were all under four (O'Brian, 2007; Pan & Jackson, 2008), thus indicating no multicollinearity. This issue of multicollinearity is important, because "A VIF measures

the amount by which the variance of a parameter estimator is inflated due to predictor variables being correlated with each other, rather than being orthogonal” (Liao & Valliant, 2012). This lack of multicollinearity is thus an indication that none of the predictor variables were correlated with each other.

**Table 2**

*PPVS-1 Descriptive Statistics for Regression Model*

<b>Variable</b>	<b><i>n</i></b>	<b><i>M</i></b>	<b><i>SD</i></b>
Privacy Violation	235	4.25	0.61
Religion and Spirituality	235	3.38	1.45
Prosocial Behaviors	235	2.83	0.69
Age	235	4.09	1.07
Years Worked in IS/IT Field	235	3.80	1.23
Consider Myself Ethical, Question 7 & 8	235	5.44	0.59
Have Had a Work Role Model or Mentor	235	4.97	1.13
Ever Had Ethics Training	235	0.66	0.47
Highest Level of Education	235	2.63	0.81
Household Income	235	4.58	1.96

**Table 3***PPVS-1 Regression Coefficients and VIFs for Privacy Violations to PII*

<b>Predictor</b>	<b>B</b>	<b>SE</b>	<b><math>\beta</math></b>	<b>t</b>	<b>Sig.</b>	<b>VIF</b>
Religion and Spirituality	-0.01	0.27	-0.02	-0.37	.709	1.31
Prosocial Behaviors	0.28	0.06	0.31	4.31	.000	1.76
Age	0.02	0.04	0.04	0.57	.567	2.04
Years Worked in IS/IT Field	0.05	0.04	0.11	1.46	.144	2.15
Consider Myself Ethical, 7 & 8	0.21	0.06	0.20	3.15	.002	1.38
Had a Work Role Model or Mentor	0.00	0.32	0.01	0.02	.982	1.15
Ever Had Ethics Training	0.04	0.07	0.03	0.52	.603	1.16
Highest Level of Education	-0.02	0.04	-0.03	-.564	.573	1.14
Household Income	0.03	0.02	0.10	1.57	.118	1.43

Statistically speaking, the results indicate that some IS/IT practitioners are less likely to commit privacy violations to PII based on their prosocial and ethical orientations. However, what does statistically significant mean in the present context? Sometime ago Cohen (1962, 1988) began working on a way to operationally define effect sizes based on their magnitude or impact of  $d$ ,  $R$ ,  $R^2$ ,  $r$ , and  $r^2$ . This is to say, Cohen mathematically sought to define these numbers with everyday standardized words. Based on Cohen's  $d$ , and its corollaries for effect sizes in  $R$ ,  $R^2$ ,  $r$ , and  $r^2$ , the behavioral sciences has come to understand  $R$ ,  $R^2$ ,  $r$ , and  $r^2$ , in terms of 0.0 to .10 as a small effect, .22 to .59 as a medium effect, and anything over .83 as a large effect. In between gaps would be represented by small to medium, and medium to large. However, Cohen (1988) cautions that "there is a certain risk inherent in offering conventional operational definitions for those terms for use in power analysis in as diverse a field of inquiry as behavioral

science” (p. 25). Nonetheless, Cohen’s standardization of effect sizes has caught on in the sciences. Based on this, it is reasonable to suggest that  $R^2$  from the regression is significantly large enough to tentatively conclude that the results be seen as optimistic, in the sense that some IS/IT practitioners are not as likely as other to commit privacy violations to PII.

However, it is nonetheless troublesome that there are those practitioners that are likely to commit privacy violations to PII. This conclusion is based on the descriptive mean score for privacy violations in (Table 2). This is to say; the mean willingness to commit a privacy violation equaled 4.25, plus or minus 0.61 standard deviations. Based on the coding scheme for privacy violation questions, which was: 1 = I would always do this, 2 = I would probably do this depending on the circumstances, 3 = I am not sure what I would do, 4 = I would probably not do this depending on the circumstance, and 5 = I would never do this, this indicates two conclusions. Minus the stated standard deviation puts some practitioners squarely in the “I am not sure what I would do” category, which was selection three on the privacy questions ratings, and others in the “I would probably not do this depending on the circumstances”, which was selection four on the privacy violations ratings. Both of these options leave open the *possibility* that a privacy violation to PII might be committed given some unknown circumstance(s). Thus, based on the current regression and the mean privacy violations scores, there is indication that IS/IT practitioners would commit privacy violations to PII.

**PII Privacy Violations Scale-2 (PPVS-2).** The PPVS-2 was comprised of the SMEs first 15 most minimally unethical privacy violations to PII (Appendix T, N, O), and Z) and, the Hallmarks Feature section (Appendix R). Appendix T lists the 15 privacy

violations used in the PPVS-2, while Appendix N displays the measures of central tendency for the privacy violations to PII, and Appendix P lists the privacy violation questions in descending values of their means. The one difference in the Hallmark Features section from the PPVS-1 was that the last question on the survey asked participants if they had participated in a similar survey within the past 30 days. A check of reliability for the intercorrelations of the 15 privacy violations to PII revealed a Cronbach of .90. This Cronbach was sufficiently below 0.95 to conclude that the privacy violation questions were not redundant.

Presented in Appendix AD are the demographics for the second survey's sample population. The participants from this survey came from Cint, USA survey services. Briefly, the PPVS-2 consisted of 172 participants. The entire sample population came from the United States. Men comprised 63.4% of the sample population, while women represented 36.6% of the sample. Overwhelming the most represented age group were individuals between the ages of 30-39, which comprised 37.8% of the sample population. The most frequently represented educational group in the sample was that of individuals with a college degree at 57.0%. One-hundred and fifteen or 66.9% of the participants identified themselves as married. When asked about children, 35.5% stated they had no children; this was followed by 23.8% with one child, and 28.5% with two children. Two groups at 19.2% equally represented the most frequent household income. These income groups were \$71,000-\$90,000 and \$91,000-\$110,000, respectively. For years of IS/IT work experience, 10-14 years and 15-19 years were almost identical at 23.3% and 23.8% respectively. Following these demographics in Appendix AD are the frequencies of job descriptors or job titles, industry certifications, and organization and association memberships which the survey participants had. Lastly, job descriptors, industry

certifications, and organization and association memberships do not total the amount of participants in the sample, because it is common for IS/IT practitioners to hold multiple industry certifications, and belong to multiple industry organizations and associations.

Because the sample N was not large enough, PCAs were not run on predictors with multiple variable questions. Instead, Cronbach alpha's were conducted on the composites of religiosity and spirituality, prosocial behaviors, and questions seven and eight from the first section of the Hallmark Features section that asks someone if they believe they are ethical. The Cronbach's for religion and spirituality, prosocial behaviors, and question seven and eight were .80, .97, and .70 respectively. Here too, as with the PPVS-1, the lower reliability score for the composite score for questions seven and eight may be attributed to the fact that only two inter-item variables were used to assess how ethical someone says they are.

The models descriptive statistics and regression coefficients are listed in Tables 4 and 5, respectively. Overall the model was weak, yet it was a significant predictor that could describe willingness to not commit privacy violations to PII at an,  $F(9, 170) = 1.99, p = .044, R^2 = .10$ . However, none of the predictors showed any significance.

**Table 4***PPVS-2 Descriptive Statistics for Regression Model*

<b>Variable</b>	<b><i>n</i></b>	<b><i>M</i></b>	<b><i>SD</i></b>
Privacy Violation	172	3.87	0.78
Religion and Spirituality	172	3.63	1.41
Prosocial Score	172	2.95	0.66
Age	172	3.87	1.22
Years Worked in IS/IT Field	172	2.78	1.37
Consider Myself Ethical, Question 7 & 8	172	4.93	0.70
Have Had a Work Role Model or Mentor	172	4.64	1.23
Ever Had Ethics Training	172	0.51	0.50
Highest Level of Education	172	2.30	0.64
Household Income	172	3.58	1.95



**Table 5***PPVS-2 Regression Coefficients and VIFs for Privacy Violations to PII*

<b>Predictor</b>	<b>B</b>	<b>SE</b>	<b><math>\beta</math></b>	<b>t</b>	<b>Sig.</b>	<b>VIF</b>
Religion and Spirituality	-0.02	0.04	-0.03	-0.43	0.665	1.10
Prosocial Score	-0.13	0.10	-0.11	-1.28	0.202	1.28
Age	0.08	0.06	0.12	1.20	0.233	1.76
Years Worked in IS/IT Field	-0.11	0.06	-0.19	-1.79	0.075	1.91
Consider Myself Ethical, 7 & 8	0.16	0.10	0.15	1.66	0.100	1.37
Had a Work Role Model or Mentor	0.00	0.06	0.01	0.08	0.939	1.34
Ever Had Ethics Training	0.03	0.12	0.02	0.27	0.787	1.11
Highest Level of Education	-0.07	0.10	-0.06	-0.69	0.490	1.17
Household Income	-0.03	0.03	-0.08	-0.99	0.322	1.23

Because the model was able to predict privacy violations to PII, but no predictor indicated significance, further investigations with a stepwise, forward, and backward regression were conducted. The stepwise regression demonstrated that age was significant at  $F(1, 170) = 10.04, p = .002, R^2 = .05$ . The forward and backward regressions demonstrated no significance. Because the stepwise  $R^2$  was as low as it was, further analysis was conducted to ensure that age was an accurate predictor. The 172 cases were split evenly into two groups of 86 cases, and then two stepwise regressions were conducted, one on the first grouping of 86 cases, and then one the second grouping of 86 cases to determine if age was a reliable predictor. The first stepwise regression came back at,  $F(1, 84) = 8.77, p = .004, R^2 = .09$ . However, the second stepwise regression in SPSS came back stating that there was no variable to put in the regression equation, thus indicating that age was not a strong enough determinant to predict privacy

violations to PII in the sample population. As troublesome as this is, it is nonetheless expected. Much literature from multidiscipline fields has been critical of stepwise regressions for decades due to the following reasons. Whittingham, Stephens, Bradbury, and Fredkleton (2006) voiced concern over parameter estimation bias, inconsistencies with the models algorithms, and lastly they state, that there is too much reliance on a single best-fit model. In fact, Mundry and Nunn (2009) squarely recommend refraining from the use of stepwise models for the following reasons. First, they are not capable of explaining a model in the global sense as regression is supposed to do, and second, they are prone to “greatly inflated Type I error rates” (p. 119), and they often include predictors that have no influence on the dependent variable. However, something had to explain why age at one point might have been a reasonable predictor, and then at another point age had no significance at all. A deeper investigation into the population sample revealed the problem. It is possible that many participants Christmas Treed survey questions, or gave the questions very little if any consideration when answering them. This supposition is based upon the following timetables to complete each PPVS (Table 6). It is clear that when examining Table 6 that there are large discrepancies in the measures of central tendency. In fact, the mean time to complete the survey for individuals taking the PPVS-2 was less than half that for the PPVS-1 and PPVS-3. Furthermore, the mode for the PPVS-2 was five minutes and twenty-six seconds. It is highly unlikely that anyone would be capable of answering the complete survey with all 68 questions in under 10 minutes. Therefore, the PPVS-2 cannot be considered a reliable measure, and therefore will receive no further attention other than brief mention in the discussion section of this research, because many participants did not respond to the survey in a responsible manner.

**Table 6***Time Tables to Complete the Three PPVSs*

	PPVS-1	PPVS-2	PPVS-3
Mean (Average)	34:28	14:32	35:30
Median	16:58	11:54	17:58
Mode	10:39	05:26	14:11

**PII Privacy Violations Scale-3 (PPVS-3).** As with the PPVS-2, the PPVS-3 was comprised of the same 15-privacy violation questions to PII, the one difference was the ending of the question, which asked the survey participant if they would commit the privacy violation if no one would know that they did it (Appendix U). The PPVS-3, in like fashion used all the same Hallmark Features questions as the PPVS-1 (Appendix R), except the last question that asked participants if they had participated in a similar survey within the past 30 days. No survey participant indicated completing a survey like this within the past 30 days. Since the ending of the privacy violation scenarios differed in the PPVS-3, a check for internal consistency was run. The returned Cronbach alpha was .89.

Presented in Appendix AF are the demographics for the third survey's sample population. Briefly, the PPVS-3 consisted of 166 participants from LinkedIn. Men comprised 141 of the participants or 63.4%, while the total women in the sample was 25 or 15.1%. The two most represented age groups were those of 30-39 years of age and 40-49 years of age, at 29.5% and 30.1%, respectively. Of the 166 participants, the largest educational group was those with only a college degree, and they represented 47.0% of the total sample population. Seventy-two point nine percent of 166 participants identified themselves as married, while the remainder said they were single. Of the 166 cases in the

PPVS-3, 31.3% percent stated that they had no children, and 27.7% said they had two children; these were the two most represented groups. The most frequent listed household income was >\$150,000 at 24.1%; this was followed by 19.9% with an income of \$91,000-\$110,000. For years of IS/IT work experience, 1-4 years and 15-19 years were the most frequently cited at 28.9% and 25.9% respectively. Following these demographics in Appendix AF are the frequencies of job descriptors or job titles, industry certifications, and organization and association memberships, which the survey participants had. Lastly, job descriptors, industry certifications, and organization and association memberships do not total the amount of participants in the sample, because it is common for IS/IT practitioners to hold multiple industry certifications, and belong to multiple industry organizations and associations.

Because the sample N for the PPVS-3 was not large enough, PCAs were not run on predictors with multiple variable questions. However, as with PPVS-1, other Cronbach's were run to ensure internal consistency for the reliability of the composite scores for religiosity and spirituality, prosocial behaviors, and questions seven and eight from the first section of the Hallmark Features section that asks someone if they believe they are ethical. The Cronbach's for religion and spirituality, prosocial behaviors, and question seven and eight came back as .80, .97, and .70 respectively. The lower reliability for questions seven and eight may be attributed to the fact that only two inter-item variables were used to assess how ethical someone says they are. All other single items predictors were individually added to the regression model.

As with the PPVS-1, the PPVS-3 was able to predict the measured lack of willingness to commit privacy violations to PII at an,  $F(9, 164) = 9.49, p = .000, R^2 = .36$ . This indicates that 36% of the variation in the criterion variable was able to be

accounted for. Based on Cohen (1988), this 36% would be considered a large effect size. The model's descriptive statistics and regression coefficients are listed in Tables 7, and 8, respectively, and the models correlation tables appear in Appendix AG. As expected, some of the predictors, and coefficients indicated that those IS/IT practitioners that score high on Hallmark Features are less likely to commit privacy violations to PII. Individuals scoring high on prosocial behaviors displayed significance at  $\beta = 0.37, p = .000$ . Similarly age showed significance at  $\beta = 0.24$ , and a  $p = .006$ , while education level was significant at  $\beta = -0.18$ , with a  $p = .006$ . This indicates that those individuals that see themselves as prosocial and that were older, were also are less likely to commit privacy violations to PII. Interestingly, while level of education was significant, it was inversely related to the willingness to commit privacy violations. This indicates that IS/IT practitioners with less education were less likely to commit these types of violations.

**Table 7***PPVS-3 Descriptive Statistics for Regression Model*

<b>Variable</b>	<b><i>n</i></b>	<b><i>M</i></b>	<b><i>SD</i></b>
Privacy Score	166	3.90	0.74
Religion and Spirituality	166	3.24	1.44
Prosocial Score	166	2.81	0.67
Age	166	3.62	1.08
Years Worked in IS/IT Field	166	2.64	1.33
Consider Myself Ethical, Question 7 & 8	166	5.28	0.68
Have Had a Work Role Model or Mentor	166	4.95	1.20
Ever Had Ethics Training	166	0.59	0.49
Highest Level of Education	166	2.25	0.78
Household Income	166	4.21	2.07

**Table 8***PPVS-3 Regression Coefficients and VIFs for Privacy Violations to PII*

<b>Predictor</b>	<b>B</b>	<b>SE</b>	<b><math>\beta</math></b>	<b>t</b>	<b>Sig.</b>	<b>VIF</b>
Religion and Spirituality	0.05	0.03	0.11	1.63	.104	1.17
Prosocial Score	0.41	0.08	0.37	4.92	.000	1.37
Age	0.16	0.06	0.24	2.77	.006	1.89
Years Worked in IS/IT Field	0.07	0.05	0.13	1.48	.140	2.07
Consider Myself Ethical, 7 & 8	0.11	0.08	0.10	1.44	.150	1.33
Had a Work Role Model or Mentor	0.01	0.04	0.01	0.26	.794	1.22
Ever Had Ethics Training	0.15	0.10	0.10	1.40	.163	1.21
Highest Level of Education	-0.17	0.06	-0.18	-2.78	.006	1.07
Household Income	0.04	0.02	0.11	1.44	.150	1.48

While the results of the regression for the PPVS-3 are encouraging, in the sense that some practitioners are less likely to commit privacy violations to PII based on their prosocial orientations, age, and level of education, it remains that there are those IS/IT practitioners that might commit privacy violations to PII. This conclusion is based on the descriptive mean score and standard deviation for privacy violations in (Table7). The mean willingness to commit privacy violations was a 3.90 and the standard deviations from the mean was plus or minus 0.74, this means that there were those survey participants that selected the privacy violation question responses of: 3 = I am not sure what I would do, and 4 = I would probably not do this depending on the circumstance. Both of these options, as with the PPVS-1, indicates that there are those IS/IT practitioners might *possibility* be willing to commit privacy violations to PII given some as of yet unknown circumstance(s).

## Summary

A series of exploratory analyses were conducted to investigate the theoretical supposition that IS/IT practitioners that identify with those Hallmark Features of moral and computing exemplars would be less likely to commit privacy violations to PII, than would be those IS/IT practitioners that did not identify themselves with the Hallmark Features of moral and computing exemplars. This hypothesis was supported. In order to make this determination, this research developed an SMEs privacy violations scale called the PPSS. This PPSS asked SMEs to rate and rank various IS/IT privacy violations in terms of which ones were, minimally, moderately, and highly unethical privacy violations to PII. From the PPSS, three PII Privacy Violations Scales (PPVS) were created that contained Hallmark Feature questions that were representative of moral and computing exemplars. For each of the three PPVSs the Hallmark Features sections were the same, except that last question of the PPVS-2 and PPVS-3 asked participants if they had previously taken a survey similar to this one within the past 30 days. Further distinguishing features were that the PPVS-1 contained the first five minimally, first five moderately, and first five highly unethical privacy violations to PII based upon the PPSS. Additionally, while the PPVS-2 and PPVS-3 asked the same first 15 minimally unethical privacy violation questions from the PPSS, the PPVS-3 further asked if an IS/IT practitioner if they would commit the privacy violation if no one were to know that they did it. This is as opposed to the PPVS-2 that ended its privacy violation question by just asking practitioners if they would commit the privacy violation to PII. All three PPVSs contained the same five-point Likert response scales of: 1 = I would always do this, 2 = I would probably do this depending on the circumstances, 3 = I am not sure what I would



do, 4 = I would probably not do this depending on the circumstance, and 5 = I would never do this.

Data was collected and analyzed from all three of the PPVSs. A determination to drop the PPVS-2 from this research was based upon two facts. There is a high suspicion that the participants from the PPVS-2 Christmas Treeed their answers, or they gave little to no consideration to the questions that they were answering. This conclusion was based on the mean time to complete the surveys (Table 6). The analysis from the PPVS-1 indicated that the overall model was a significant predictor for willingness to not commit privacy violations with an effect size of  $R^2 = .32$ . This indicated that some of the predictors could explain 32% of the variability in the dependent variable. The individual predictor results validated that those IS/IT practitioners that identify themselves as having prosocial orientations and being ethical individuals were less willing to commit privacy violation to PII, than those IS/IT practitioners that did not identify with these two dispositional elements of moral and computing exemplars.

However, the other seven of the nine predictors did not demonstrate that they could account for any of the variability in the dependent variable. Similar to the PPVS-1, the overall model of the PPVS-3 demonstrated that it was able to predict a lack of willingness to commit privacy violations at an  $R^2 = .36$ . Thus, some of the predictors explained 36% of the variability in the dependent variable. In this case it was those IS/IT practitioners that identified themselves as having a prosocial orientation that were less willing to commit privacy violations to PII than were those practitioners who did not identify with this orientation. Additionally, age also represented one predictor that determined a lack of willingness to commit privacy violations to PII. This can be interpreted as, those individuals that are older, were less willing to commit these

violations. Lastly, education also proved to be a significant predictor for those less likely to commit these types of IS/IT violations. However, the results indicated that less and not more education was the predictor to not committing privacy violations.

In conclusion, the effect sizes of both regressions proved to be large enough (Cohen, 1988) to conclude that both the PPVS-1 and the PPVS-3 were in part able to explain a significant amount of which IS/IT practitioners might be less willing and more willing to commit privacy violations to PII. However, not all predictors of the PPVS-1 and PPVS-2 demonstrated significance.

## Chapter 5

### Conclusions, Implications, Recommendations, and Summary

#### Introduction

This chapter presents a summary of findings based upon the hypothesis for this research. Conclusions are discussed in terms of the goals set for this research, analyzes performed, and the results that were achieved. In addition, strengths, weaknesses, and limitations of the study's finding are presented. Moreover, explorations for this study's impacts to the field of information privacy and security are discussed, along with how this research may impact future research. Recommendations for future research and considerations for organizational practices in training and personnel selection are considered, as are recommendations for the further development of this instrument. Lastly, this chapter closes with a summary of all processes and procedures that went into this research.

#### Conclusions

As a reminder to the reader, the data from the PPVS-2 is not addressed in most sections of this chapter. This is because many of the participants either Christmas Treed their responses or gave little to no consideration to the questions that they were responding to. Therefore, it was determined that many of the responses were either falsified or inaccurate. This assessment is based on the average time to completion on the PPVSs (Table 6). Consequently, it is only reasonable to expect that no interpretations or conclusions can be drawn from the PPVS-2. However, the rationale for developing and

implementing the three surveys does deserve some attention. Since the PPVS-1 made use of the widest spectrum of privacy violation questions, and given that practitioners were willing to commit these violations, it made sense to investigate what the practitioners would do with less severe privacy violations. Since the practitioners were willing to commit even less severe privacy violations, it stood to reason that no one would intentionally do something wrong with the perception of getting caught. Therefore, the PPVS-3 asked the same privacy question as the PPVS-2, but with the distinction that the practitioners knew that no one knew that they had committed the violation. Thus, the PPVS-2 was designed to act as a conduit to the PPVS-3, which presented the most reasonable real-world situation, in that it is highly unlikely that someone would commit a violation with the knowledge that they would get caught.

Driving this exploratory and theoretical research was the following hypothesis.

Are IS/IT practitioners who identify themselves as possessing some of the predictive measures of the Hallmark Features that moral and computing exemplars have, less likely to commit privacy violations to PII, than those IS/IT that do not identify as possessing some of the Hallmark Features of moral and computing exemplars?

Nine predictor variables helped determine the validity of the hypothesis. The nine-predictor variables for this research were the composite score for religiosity and spirituality, and the composite score for prosocial behaviors. Additionally, questions seven and eight from the first section of the Hallmark Features section were selected because they helped identify if an individual considered themselves ethical. Lastly, age, level of education, household income, years worked in the IS/IT field were also selected, and whether a practitioner had ever had any type of ethics training, along with whether or

not someone said that had had a career moral mentor. The information to follow is presented in terms of the regressions run for the PPVS-1 and PPVS-3, and then for each of the predictors relative to each PPVS.

Based upon the regressions that were run on the PPVS-1 and the PPVS-3, evidence strongly suggested that some practitioners were less willing to commit privacy violations than were other practitioners; this is based upon some practitioners' identifications with various moral and computing Hallmark Features. Therefore, it is reasonable to suggest that there are moral motivations, and other factors that influence decision-making relative to being less willing to commit privacy violations to PII. Comprehensively the PPVS-1 and PPVS-3 displayed an  $R^2 = 0.32$ , and an  $R^2 = 0.36$ , respectively. Of the nine predictors, prosocial orientation dominated the significant results found in both the PPVS-1 and PPVS-3. Prosocial orientation displayed a level of significance for the PPVS-1 at a  $\beta = 0.31$ , and  $p = .001$ , and for the PPVS-3 at a  $\beta = 0.37$ , and  $p = .001$ . Individually, on the PPVS-1 the other predictor that demonstrated significance was the composite question of seven and eight from the first section of the Hallmark Features section, which asked an individual how ethical they believed they were. This ethics question came back with  $\beta = 0.20$ , and  $p = .002$ . Other than prosocial orientation on the PPVS-3, age showed significance with a  $\beta$  of 0.24 at  $p = .006$ , and education showed significance with a  $\beta = -0.18$  at  $p = .006$ . No other predictors came back showing any significance in either the PPVS-1 or the PPVS-3.

Comparatively speaking, it is difficult to assess the findings of this research, both significant and not significant relative to other pieces of literature, given that this research stands on its own in the field of IS/IT privacy and security and moral decision-making. This same conclusion can be drawn relative to other fields of research, because to date no

other discernable literature such as this one appears to exist. Therefore, consensus, or lack thereof it for these findings must be discussed proximate to individual findings of other research unrelated to information privacy, the severity of privacy violations, and the willingness to commit unethical privacy violations to PII in the IS/IT field. This is because a singular, clear descriptive and uniform body of knowledge to help understand unethical decision-making behaviors in an IS/IT context as related to the privacy violations to PII does not exist. Thus, it is best to understand the conclusions, implications, and recommendations of this research from a theoretical and multidisciplinary perspective. In this manner, a more well-rounded explanation is possible that allows for greater depth and breadth of understandings. Additionally, what corollaries that can be drawn, are somewhat speculative, and theoretically derived, yet nonetheless valuable to the interpretation of the body of knowledge that this research created.

Much literature discusses the role of religiosity, ethical judgment, and ethical behaviors in organizational settings. However, as Parboteeah, Hoegl, and Cullen (2007), Walker, Smiter, and DeBode (2011), and Weaver and Agle (2002) have noted, past literatures suggest mixed results, and because of this, the directions and magnitudes of interaction between religion, ethical judgment and organizational behavior has remained elusive. Similarly, spirituality, ethics, and the workplace have also garnered considerable attention in recent decades. However, as with religiosity, ethics, and workplace behaviors, Gotsis and Kortezi (2007) have noted that spirituality, ethics, and organizational judgment and behavior are “full of obscurity and imprecision...” (p. 575). In addition, even though literature from Hardy, Walker, Rackham, and Olsen (2012), Walker (2003), Walker and Frimer (2008), clearly indicate an association between ethical

behavior, religiosity and spirituality, this connection has been via moral exemplar's behaviors, and this research had no exemplar sample population to work with. Nevertheless, Walker and Frimer also caution that the relationships between religion, spirituality, and exemplarity, or highly ethical behaviors, are likely complex and interwoven with possibly other constructs. If in fact these factors are likely to interweave with others, it is possible that because the necessary other factors were not present, it made finding these interactions just that much harder, which is a possible reason that religion and spirituality showed no significance on either the PPVS-1 or PPVS-3. In other words, multiple factors come into play when determining the reasons for moral motivations (Blasi, 1980, 1983), especially when examining religiosity, spirituality, and ethics.

As expected, prosocial orientations on both the PPVS-1 and PPVS-3 demonstrated strong statistical significance. The association between ethical behavior and prosocial orientations is well established in the annals of exemplar literatures (Colby & Damon, 1992; Huff et al., 2008a, 2008b; Huff & Frey, 2005; Matsuba, & Walker, 2005; Oliner & Oliner, 1988; Walker & Frimer, 2007, 2009; Walker, 2014). Furthermore, ethical behaviors and prosocial orientations have been demonstrated to have strong ties within organizational frameworks (Chiu, 2003; Dozier and Miceli, 1985; Hannah, Avolio, & Walumbwa, 2011; Miceli, Near, Rehg, and Van Scotter, 2012). In this sense, prosocial behaviors can be seen as internal moral motivations directed at helping others, much like doing the right things for the right reasons. Based on this well established understanding of prosocial behaviors, it is only logical that those IS/IT practitioners that identified themselves as having prosocial orientations were less willing to commit privacy

violations to PII, than were those practitioners that did not identify themselves as having strong prosocial orientations.

The next predictor in the regression models for the PPVS-1 and PPVS-3 was the composite question of seven and eight from the Hallmark Features first section. These two questions together measured how ethical IS/IT practitioners thought they were. For these two questions survey participants responded to question seven, which asked “My integrity at work is paramount to who I am as a person, and how my peers see me”, while question eight asked “I consider myself a steward of social responsibility in your career.” The possible responses were as follows: Strongly disagree, Disagree, Somewhat disagree, Somewhat agree, Agree, and Strongly agree. Given that those practitioners that identified themselves as having prosocial orientation were less willing to commit privacy violations due to their ethical nature, it would only make sense that the composite of questions seven and eight also demonstrate significance if a practitioner indicated that they were less willing to commit privacy violations to PII. This is consistent with Hannah et al. (2011) who have demonstrated that prosocial orientation and ethical behaviors correlate. However, this finding occurred only with for the PPVS-1 model, and not the PPVS-3. One, and quite possibly the most reasonable conclusion for this finding is that the PPVS-1 never left open the possibility that the IS/IT practitioner would never get caught committing the violation, whereas the PPVS-3 did. In other words, the manner in which the privacy violation questions ended between the PPVS-1 and PPVS-3, were completely different. While the PPVS-1 asked participants how likely, they were to commit each of the privacy violations; the PPVS-3 asked participants how likely they were to commit the privacy violations *if no one would ever know that they would commit the violation*. Realistically, it is reasonable to conclude that most individuals would not commit these



types of violations if they thought that they were going to get caught, but if they knew they would not get caught, they very well might commit the violation to PII. After all, most people commit wrongdoings with the perception that they will not get caught, or hope that they will not. Therefore, between the PPVS-1 and PPVS-3, the PPVS-3 most likely represents real world scenarios. However, another possible interpretive explanation remains that cannot be addressed. The PPVS-2 was meant to act as a conduit between the PPVS-1 and PPVS-3, but due to the problems that plagued the PPVS-2, accurate data is not available. The PPVS-2 would have acted as a conduit or bridge to understanding and interpretation in the following manner.

The first 15 privacy violation questions used on the PPVS-1 were completely different from the 15 privacy violations on the PPVS-2 and PPVS-3. The PPVS-1 used the five most minimally unethical, five most moderately unethical, and five most highly unethical privacy violations to PII that were based on the SMEs ratings and ranking of all privacy violations (Appendix P and Appendix S). This is as opposed to the 15 most minimally unethical privacy violations that were used on the PPVS-2 and PPVS-3 (Appendix P and Appendix S). Both the PPVS-1 and PPVS-2 ended the privacy violation questions in the same manner; participants were asked how likely they were to commit the privacy violation. However, the PPVS-3 ended each privacy violation question in the following manner; "If no one would ever know that, you would commit the violation would you do it." Testing the willingness to commit privacy violations in this manner was not only a matter of the privacy violation, but also how the questions ended. If the PPVS-2 had demonstrated significance for the composite of question seven and eight, it would have meant that those individuals that saw themselves as ethical were less willing to commit privacy violations to PII. Additionally, more conclusive support for the

supposition that, knowledge of not getting caught committing an unethical behavior might very well be a determining factor for whether an IS/IT practitioner would commit the violations.

The next four predictors for the PPVS-1 and PPVS-3 were age, level of education, household income, and years worked in the IS/IT field. In part, these predictors were selected due to the theoretically based and exploratory nature of this research, and in part because literatures have demonstrated some theoretical, anecdotal, and statistical grounded relevance that connects moral reasoning and ethical behavior to these predictors. For instance, as one ages, moral reasoning and decision-making become more mature as noted by higher scores on the DITs (Mujataba, et al., 2009; Rest et., 1999; Rest, Thoma, Narvaez, & Bebeau, 1997). Higher scores are also indicators of more advanced principled reasoning. Furthermore, higher levels of moral maturity are known to correlate with higher level of education, and more advanced age (Bebeau & Monson, 2008; Freeman, 2007; Mobley, 2002; Rest, Davison, & Robbins, 1978; Rest, Narvaez, Bebeau, & Thoma, 1999; Thoma, 2006). That is to say, older more mature individuals, sometimes with more advanced levels of education, especially in professional careers where ethics are a concerned (Bebeau, 2002b; Huff & Rogerson, 2005) are also likely to present with higher and more mature moral reasoning and decision-making skills. The rational for this is that, principled moral reasoning, like that of exemplars, generally promote ethical integrity, (Miller & Schlenker, 2011; Narvaez & Lapsley, 2009a), particularly in business environments (Trevino, 1986; Trevino & Brown, 2004). Additionally, Cannon (2001) demonstrated that those individuals with more years of work experience also showed slightly higher levels of moral reasoning, and thus possibly also ethical behavior; however, only limited literature documents this type of relationship

(Mujataba, Cavico, McCartney, DiPaolo, 2009). Additionally, it stands to reason, if only anecdotally, that a higher level of income might also track with a higher level of education, which may also correlate with individuals of more advanced age. The rationale for this is that often with more education, comes advanced age, and as one ages with more education, they also progress up the career ladder, which leads to higher income. Therefore, it was anticipated that age, level of education, and years of career experience may be influential in an IS/IT practitioners willingness to not commit privacy violations to PII.

In the final analysis of the PPVS-1, age, level of education, household income, years worked in the IS/IT field turned out to be significant. However, for the PPVS-3, age and education were significant predictors, but not income or years worked. Overall, these results are not surprising. With regards to the PPVS-1 and PPVS-3, much statistically significant literature over the decades support the association that with more advanced age and more advanced education comes higher levels of moral maturity (Bebeau, 2008; Mujataba, et al.; Rest et., 1999; Rest, Thoma, Narvaez, & Bebeau, 1997; Trevino, 1986; Walker, 1986; You, Maeda, & Bebeau, 2011). However, moral maturity is not, nor has it been identified in the literature as the end all be all precursor to ethical behavior. Case in point, Bebeau (2012) a noted researcher in moral maturity and judgment, and the professional field of dentistry, has previously identified numbers of dentists who have committed unethical acts. In fact, evidence by Bebeau (2008), Grady et al. (2008), and many others have suggested, that what makes the difference is ethics training in the professions. The conclusion that moral maturity, age, and education do not necessarily equal good behavior should be self-evident from the results of the PPVS-1. However, lack of significance for age in the PPVS-1 may have been masked by some

other unseen determinate that was not measured because age did come back significant in the PPVS-3. Although, this interpretation that age may mean something relative towards a less willing attitude towards committing privacy violations to PII in the results of the PPVS-3 needs to be approached with caution. The amount of variance that was explained by age in the PPVS-3 was  $\beta = 0.24$  at  $p = .006$ ; at best this is a very small effect especially given the size effect tables of Cohen (1988). Similarly, while education was not a significant predictor with the PPVS-1, it was with the PPVS-3. The question is why did the relationship between education and a less willing attitude towards committing privacy violations comeback negative with a  $\beta = -0.18$ , and  $p = .006$ . Again, at best the interpretation must be approached cautiously because of the significance value. Clearly, this means that practitioners with less education are less willing to commit privacy violations to PII. Keeping in mind that moral maturity and moral reasoning are not direct indicators of moral action or ethical behavior (Blasi, 1980, 1983; Shao, Aquino, & Freeman, 2008), what can be said? Decades of literature once supported Kohlberg's stages of moral development, however, with the development and decades of research that have gone into the DITs, it is wise, if not even prudent to realize that myriad factors play towards an individual's moral motivations, that very well may not have been captured in this research. Similarly, looking back at the PRIMES model (Huff et al., 2008a, 2008b) this notion of multiple factors acting upon moral action becomes even more evident. For instance, Roberts and Mroczek (2008) note that stage of life can make a difference, while Huff et al. (2008b) and Lucas and Donnellan (2009) mention that conscientiousness is also a factor in moral motivation. Moreover, while no currently discernable literature gives rise to this speculation, a certain attitude for those with less education may explain why they would be less willing to commit privacy violation to PII.

Those practitioners with less education may not have been taking the privacy violation questions at face value. That is to say, those individuals with less education may have answered in a manner that they thought was prosocial, which means they answered the way that they thought society would want to see them, not as they actually are. By the same token, those individuals with more education may have rationalized a thought similar to “I am too smart to get caught, so of course I would commit the violation.” After all, most people do not do unethical things with the perception that they will get caught. Another explanation may simply lay in the fact that those IS/IT practitioners with more education were simply willing to commit privacy violations to PII, because the ending of the privacy violation questions on the PPVS-3 asked, “If no one could ever find out that you did this, what would you do?” Therefore, without significant further follow-up studies it is wrong, if not also irresponsible, to speculate over the causes for the education interaction effect given the extremely small effect size.

The fact that both years worked in the IS/IT field and household income came back insignificant on the PPVS-1 and PPVS-3 is not surprising. Even though Cannon (2001) showed, a slight significance between years worked and moral development, the literature did not measure intent to act, which this research attempted to tap. However, one might speculate that the power of higher salary would act to deter unethical behavior and prompt more ethical action in the face of getting caught at commit a privacy violation, and possibly losing one’s job. Similarly, any anticipation that household income would show significance was at best, merely a speculation based on the predictors of age, and education displaying strong size effect on both the PPVS-1 and PPVS-3. However, because moral motivations to act ethically have so many predictors that can influence it, it is virtually impossible to say what predictors may have helped

income and years worked display significance. Three notable examples are the works of Cronan and Douglas (2006, 2008), Leonard and Cronan (2001), and Leonard, Cronan, and Kreie (2004) who explain that things like normative beliefs, organizational ethical climate, ego strength, gender, locus of control, and cultural relativisms among other items, all play on behavioral intention to act ethically. Similarly, as Huff et al. (2008a, 2008b) noted with their computing exemplars, personality, the integration of morality into a self-system, moral ecologies, and skills and knowledge also contribute to whether and how IS/IT practitioners act ethically.

The last two predictors used to determine if IS/IT practitioners were less willing to commit privacy violations to PIII were whether or not they had had any fashion of ethics training, and whether or not they had ever had a moral role model at work, like a moral mentor. Neither of these predictors demonstrated any significance on the PPVS-1 or PPVS-3. That ethics training came back with no significant results, is not a total surprise. There is certainly no dearth of literatures addressing ethics training and ethical behavior. However, great discrepancies across these pieces of literature do exist. For example, Bebeau (2008), Bebeau and Monson (2012), Davis (2009), Grady et al. (2008) provide evidence that ethics training in the professions, that is to say fields where certifications and licensing may be or is required, has positive effects on ethical behavior. Contrary to the above, Baykara, Demir, and Yaman (2014) showed that ethics training of nurses in some instances does not help. Two facts deserve attention. First, IS/IT practitioners are not professionals in the sense that there is a single governing body that mandates a code of ethics, and that can place sanctions on these individuals, such as with doctors, attorneys, pilots, engineers, and accountants. Therefore, if practitioners were governed by a sanctioning body that required ethics training it may then have been that

the predictor of ethics training may have come out being significant. In all, it is important to remember, that the motivations towards ethical action are often influenced by other factors, and any number of these factors were not addressed in this research.

The last predictor to be used in this research was that of whether or not an IS/IT practitioner said that they had had a moral mentor. While the majority of responses for both the PPVS-1 and PPVS-3 indicated that they somewhat agreed to fully agreed to having a moral work mentor, this was not a significant predictor towards a lack of willingness to not commit privacy violations. If this research had a population of working computing exemplars to compare to, the results may have been different, and comparatively running t-tests to test the mean difference would have likely been able to determine if a moral mentor truly makes a difference. This speculation is based upon the fact that in almost all instances of research with exemplars that examine their life story narratives, exemplars state that they have had someone in their lives that helped shape and influence their moral motivations. However, this research was not working with an exemplar population, and the best that might be said of those practitioners that stated that they have or had a moral mentor is that, the mentor was likely not as influencing as they are with exemplars. This is understandable in that exemplars are a composite of their dispositional parts, and so too are non-exemplar computing practitioners. In this instance, the ethical parts of a moral mentor did not outweigh the unethical parts, or so it would appear. Alternatively, for many people morality is subjective, so what the practitioners thought to be a moral mentor may not have been by standards set in various pieces of other literature (Brown, Trevino, & Harrison, 2005; van Dierendonck, 2010), or by the standards of other individuals.

In sum, while this research did find significant findings, there are items such as strengths, weaknesses, and limitations that need to be addressed. First and foremost, the goal of this research, which was to develop, implement, and validate a new instrument that was capable of determining which IS/IT practitioners were less willing to commit privacy violations to PII based on a set of Hallmark Features that are known to associate with moral and computing exemplars; this goal was achieved. A further strength of this research is that it is the first of its kind, which means entire bodies of uncharted literature can be developed from it in the areas of personnel selection and testing within the IS/IT fields. Additionally, with further development, this instrument can aid organizations in identifying training areas within IS/IT privacy and security, so that internal policies, and federal compliance laws are met. Moreover, with additional development, this instrument could be used to reach across cross-cultural lines due to the fact the sample populations were not only U.S. based, but also included an international sampling of IS/IT practitioners. However, before these types of achievements are attained, certain weaknesses and limitations inherent to the design, structure, and implementation of the instrument must first be resolved and then verified that they have been overcome.

Greater depth and breadth are needed for the predictors so that each of the predictors is capable of more accurately measuring multiple factors per predictor. This was a major shortcoming and limitation in the design of the survey instrument. Had each of Hallmark Section contained more questions, it might have been possible to extract multiple factors in each section through Principle Components Analysis. Thus, a more well-rounded instrument would have been developed. The construction of the Ethics, Training, and Awareness section within the Hallmark Features section placed too great of a reliance on understanding codes of ethics and ethics training of practitioners, and not



enough emphasis was given to more fully developing sets of question that would have more accurately measured how ethical IS/IT practitioners actually thought they were. The predictor of household income needs to be disposed of, and replaced with what the practitioner's salary range is. The instrument was ever meant to measure what a spouse or significant other contributes. Measuring an individual's salary might very well have been a more tell tail indicator of whether or not they would commit a privacy violation to PII. A restructuring of the religion and spirituality section should be considered in an effort to determine if these items truly have no predictive quality for this type of instrument. Expansion of the career or job section is necessary, because many participants added descriptors under the OTHER category that were not listed. Moreover, a wider range of security and privacy positions could have been included for more refinement and later statistical analyzes. One inherent limitation that was also a weakness of design and methodology was that no attention was directly paid to IS/IT practitioners industry certifications and organization and association memberships. It is quite possible that practitioners that hold certain industry certifications and that belong to specific organizations or associations are likely to be more ethical than practitioners that do not hold certain certifications or belong to certain organizations or associations. The reasoning behind this is that certain certifications, and organizations and associations are held in very high regard, and often take quite a large amount of time to attain. This is especially true for certain privacy and security based certifications and organization or association memberships. To attain these items requires rigorous training, the acceptance of organizational codes of ethics, testing on these ethics, and continuing education credits. Therefore, it is quite possible that had these items had been closely examined, significant results may have shown that practitioners that have attained these standards

would be less willing to commit privacy violations to PII. Even though age and education showed some significance, the effect size was small, and this may have been limited by sample sizes, thus a weakness and limitation found in this research was possibly also sample size. Overwhelmingly, the greatest weakness, and the most significant limitation was the difficulty that was encountered with the mean time to complete the PPVS-2. Had survey participants not Christmas Tree responses and given more consideration to the questions being asked, this entire survey sample would likely not have to have been dropped from this study. Without the data from the PPVS-2, no comparative analyzes were able to be run against the PPVS-3.

### **Implications**

The overall implications of this research are not only interesting, and troubling, but they are also contributory to the field of information privacy and security for the following reasons. In his now seminal paper, Mason (1986) cautioned that information privacy would be of significant concern in the future. Among many others, Martin and Woodward (2011), and Woodward, Davis, and Hodis (2007) have demonstrated that IS/IT students display difficulties in identifying ethical issues, and thereby have difficulty making the correct ethical judgments. If today's IS/IT students are tomorrow's practitioners, which they are, then society as it appears, is going to be in an even more troubled state with information privacy than it already is. This clearly resonates with the findings of Kuo et al. (2007), who identified that male IS/IT practitioners have a lower self-efficacy for protecting information privacy than do female IS/IT practitioners, and that females have a higher self-efficacy for the non-acquisition of PII. Similarly, Kuzu (2009), revealed that "ICT professionals" (p. 91) were not sure how to define computer

ethics, and often did so in terms of citing immoral computing behaviors. It is no doubt, that at least, in part due to these difficulties, that Woodward (2007) and Huff et al. (2008b) have called for an instrument to measure the intermediate ethical conceptualizations of IS/IT. In fact, Huff et al. (2008b) specifically makes mention for the type of privacy-based instrument that this research developed. Therefore, this research contributed to the body of knowledge that was looking for a way to measure one of the difficulties that society faces with PII. This research also indirectly validated a supposition of Huff et al. (2008a, 2008b), in that, it was able to demonstrate that IS/IT practitioners that more closely identified themselves with some of the components of moral and computing exemplars were less willing to commit privacy violations to PII. The importance of this cannot be understated. The PRIMES model that Huff et al. (2008a, 2008b) created was theoretically based on statistically grounded research, yet no one had ever found direct statistical support for the PRIMES model until this research. Additionally, less than a paucity of literature out there that ever attempted a theoretical and practical way to define the severity of privacy violations to PII, in fact, this may be the first research of its kind. Therefore, the possible impact to the field of information privacy is wide open. Moreover, Belanger and Crossler (2011) noted that:

The review of the literature reveals that information privacy is a multilevel concept, but rarely studied as such. We also find that information privacy research has been heavily reliant on student-based and USA-centric samples, which results in findings of limited generalizability... We call for research on information privacy to use a broader diversity of sampling populations, and for more design and action information privacy research

to be published in journal articles that can result in IT artifacts for protection or control of information privacy (p. 1017).

Thus, this research also contributed to the field of information privacy in that it used populations of working IS/IT practitioners that were not just based in the USA, but also internationally. Lastly, this research observed that IS/IT practitioners who display a cohesive disposition towards prosocial behaviors were less likely to commit privacy violations to PII. This finding, and its contribution, is something new to the field of information privacy and ethics in IS/IT, as such, it has created a new body of knowledge in the privacy of PII, that was never present prior to this research.

### **Recommendations**

The prosocial disposition of IS/IT practitioners said a lot for how they would access and disseminate PII. Prosocial dispositions represent one component of personality (Brief & Motowidlo, 1986; Penner, Fritzsche, Craiger, & Freifeld, 1995), many other components exist, though not all personality profile inventories use the same name for personality components, or test for all of the same personality components. It is highly probably that other components from other personality and personnel profile inventories, if extracted properly could be used, as determinants for which IS /IT practitioners are less willing to commit privacy violations to PII. Therefore, future research must attempt to do this, so that organizations have a tool to assess which practitioners need more sensitivity training so that they respect PII, or to determine which practitioners should not be hired in the first place. In a manner of speaking, the initial development of the PPVS was to support the further development of a more inclusive personality profile inventory. This type of inventory can then specifically be

administered to IS/IT practitioners to determine if they fit the personnel profile of an individual that would with respect guard information privacy, and that would not commit violations to federal compliance acts, standards, policies, and regulations that impact an organizations IS/IT environment. Provided in Table 9 is a list of personality markers that should be investigated in the future, because they may provide insight into which IS/IT practitioners are the most conscientious towards protecting information privacy, and they are the most frequently identified markers of personality characteristics on personality and personnel inventories.

**Table 9 Components of Personality Markers to Measure**

Accountability	Ethical leadership	Prudence
Adherence to ideals	Fairness	Purposefulness
Agreeableness	Honesty	Reflection
Altruism	Honor	Respect
Attention to detail	Impulse control	Respect for authority
Caring & Care Taking	Impulsiveness	Responsibility
Cautiousness	Influence	Risk taking
Civic mindedness	Integrity	Self-regulation
Compassion	Justice	Social responsibility
Compliance	Kindness	Strategic thinking
Competence	Law abidingness	Trustworthiness
Conscientiousness	Negativity	Understanding outcomes
Cooperativeness	Objective & Logical reasoning	Understanding rules & order
Dominance	Opened to experience	Volunteerism

Dutifulness                      Openness to correction

Empathy                          Positive emotions

Additional recommendations include but are not limited to, expanding the severity of privacy violation questions, and also including general and specific violation questions that revolve around the security of IS/IT. Specifically, an entire battery of questions could be developed for the individual domains found within the IS/IT field. Areas such as databases, data mining, big data, wireless communications, auditing, email, passwords, and a myriad of others should be considered. Additionally, questions from the above-mentioned domains should be focused on the policy and compliance areas of PCI-DSS, SOX, FERPA, HIPAA, and HI-TECH, because it is here that some of society's most sensitive information is located. Should the aforementioned recommendations be developed and implemented, the results of findings could then be targeted to in-house organizational training awareness. Lastly, while the importance of understanding working populations of IS/IT practitioners privacy and security behaviors cannot be understated, it would be interesting to run some modification of the PPVS-3 with undergraduate and graduate IS/IT students.

### **Summary**

Evidence suggests that IS/IT practitioners are known to commit questionable and often unethical behaviors within their fields of practice (Cyber-Ark, 2009, 2011; Kuo, Lin, & Hsu, 2007). Chung and Khan (2008) noted that not all unethical IS/IT behaviors carry the same impact in terms of severity. However, Huff et al. (2008a, 2008b) have noted that there are some IS/IT practitioners, namely moral computing exemplars, that due to the virtuous features of their dispositions, may not be as willing to commit

unethical acts within their career domains. Therefore, the research in this dissertation investigated whether those IS/IT practitioners that identify with some of the Hallmark Features of moral and computing exemplars would be less willing to commit privacy violations to PII, than those IS/IT practitioners that did not identify with the Hallmark Features of moral and computing exemplars. The willingness to commit these privacy violations was based on their severity. In order to determine if this hypothesis was valid, the follow study was conducted.

A group of SMEs assessed the severity of 40 privacy violations to PII. From these rating and rankings, three surveys were developed that were administered to IS/IT practitioners. Each of the surveys contained a five-domain Hallmark Feature sections with questions that were theoretically meant to determine if these practitioners would identify with the features of moral and computing exemplars. The five sections were Career and Organizational Values, Religion and Spirituality, Ethics Training and Awareness, Prosocial Behaviors, and General Demographics. From these sections, nine predictors were selected. Three of the predictors were the composite scores of religion and spirituality, prosocial behaviors, and question seven and eight that asks how ethical a person thinks they are. The remaining predictors were age, years worked in the IS/IT field, whether practitioners have had a moral work mentor, if they had ever taken ethics training, level of education, and lastly household income. In addition to the Hallmark Features section, each survey contained 15 privacy violation questions that survey participants responded to in terms of the willingness to commit these violations on a five-point Likert scale. The IS/IT practitioners surveys were known as the PII Privacy Violations Scale (PPVS), and were designated from each other by the number one, two, or three at the end of it. The PPVS-1 was comprised of the SMEs five most minimally,

five most moderately, and five most highly unethical privacy violations to PII, and the Hallmarks Feature section. The PPVS-2 was comprised of the SMEs first 15 most minimally unethical privacy violations, and the same Hallmark Feature questions except the last question asked participants if they had participated in a similar survey within the past 30 days. The privacy violation questions on both the PPVS-1 and PPVS-2 ended in the same manner; by asking the participants how likely, they would be to commit the privacy violation on a five-point Likert scale. The PPVS-3 used the same Hallmark Features section as the PPVS-2, and the same 15 privacy violation questions. Except in the case of the PPVS-3, the privacy violation question ended by asking participants if they would commit the privacy violation to PII if no one knew that they did it.

Due to questionable issues of validity with the PPVS-2, it was removed as a factor in determining the validity of the hypothesis for this research. However, both the PPVS-1 and PPVS-3 remained relative to this study, and were used in the final analyses and conclusions. Both sample populations were comprised of working IS/IT practitioners and both samples contained international and USA survey participants. The overall model for both the PPVS-1 and PPVS-3 proved to be a significant predictor for those IS/IT practitioners that were less willing to commit privacy violations to PII based upon some of the Hallmark Features of moral and computing exemplars. The findings from the regression that was run on the PPVS-1, indicated that individuals with higher prosocial orientation scores and higher scores on the composite question of seven and eight were less willing to commit privacy violations to PII than were those practitioners that scored lower on these two items. Similarly, prosocial orientation was significant on the PPVS-3. Practitioners scoring higher on prosocial behaviors were less willing to commit privacy violations to PII than were those practitioners that had lower prosocial orientation scores.



However, unlike the PPVS-1, the composite question of seven and eight did not prove to be a significant predictor. Although, age and education demonstrated significance on the PPVS-3, both displayed a very small size effect, and education had a negative effect, which means that individuals with less education were less willing to commit privacy violations.

Overall, this research confirmed that there are those IS/IT practitioners that are more and less willing to commit privacy violations to PII. Note that in the previous sentence the words “would never commit a privacy violation” were never used. While this research indicated that some practitioners were statistically less inclined to commit privacy violations based upon certain factors, it was never the cases where PII privacy violations would never take place. This is alarming, because practitioners are clearly not acting ethically in terms of their Role Specific Obligations (RSOs) to the Intermediate Concepts (ICs) of PII privacy. This can easily present a problem, because these so-called guardians of sensitive information certainly are not demonstrating any understanding with regards to the potential psychological or financial impact that their behaviors may exact upon another. It makes one wonder, are some IS/IT practitioners even aware of what their RSOs are towards the ICs of privacy. If these individuals are not aware of their obligations, then they are less likely to act ethically. The question then becomes, how do organizations instill more virtuous qualities of character in their IS/IT practitioners so that members of society have less fears over their PII being accessed without authorization, and also not be concerned that their PII might illegally be disseminated. This is not only a concern for members of society, but also organizations. What is at risk for the organization is not only the possibility of federal fines and sanctions for privacy violations, but also their reputation that society has for them.

As previously stated, the purpose of this research was an initial theoretical exploration of which Hallmark Features distinguish which IS/IT practitioners as being less willing to commit privacy violations to PII. Despite a number of earlier stated weaknesses and limitation in this study, this research was able to draw valid conclusions based on significant findings, therefore, further investigations are warranted to determine what other Hallmark Features can distinguish IS/IT practitioners that are less likely to commit privacy violations to PII, especially in the absence.

**Appendix A – Aristotle’s 12 Virtues, Vices, and Deficiencies**

Sphere of Action or Feeling	Excess (Vices)	Mean (Virtue)	Deficiency (Vices)
Fear and Confidence	Rashness	Courage	Cowardice
Pleasure and Pain	Self-indulgence	Temperance	Insensibility
Getting and Spending (major)	Prodigality	Liberality	Illiberality/Meanness
Getting and Spending (minor)	Vulgarity/Tastelessness	Magnificence	Pettiness/Stinginess
Honor and Dishonor (major)	Vanity	Magnanimity	Pusillanimity
Honor and Dishonor (minor)	Ambition/Empty vanity	Proper ambition/Pride	Unambitiousness/ Undue humility
Anger	Irascibility	Patience/Good Temper	Lack of spirit/ Unirascibility
Self-expression	Boastfulness	Truthfulness	Understatement/ Mock modesty
Conversation	Buffoonery	Wittiness	Boorishness
Social Conduct	Obsequiousness	Friendliness	Cantankerousness
Shame	Shyness	Modesty	Shamelessness
Indignation	Envy	Righteous indignation	Malicious enjoyment/ Spitefulness

*Note.* Adapted from Aristotle (1955). *The Ethics of Aristotle: The Nicomachean Ethics* (rev. ed.) (J. A. K. Thomson, trans.) New York: Viking Press.

### Appendix B – Neo-Aristotelian Virtues

Autonomy	Curiosity	Hope	Prudence
Attentiveness	Civic mindedness	Helping	Passion
Articulateness	Compassion	Integrity	Persistence
Agreeableness	Conscientiousness	Independence	Religiousness
Amiability	Determination	Justice	Reflective
Ambition	Forgiveness	Kindness	Responsibility
Ability	Faith	Loyalty	Saintliness
Altruism	Fairness	Love of learning	Self-regulation
Bravery	Focus on quality	Love	Spirituality
Creativity	Gratitude	Leadership	Social-intelligence
Courage	Graciousness	Modesty	Temperance
Cooperativeness	Generosity	Moral imagination	Trustworthiness
Contentment	Humility	Moral creativity	Truthful
Competitiveness	Honor	Open to experience	Tolerance
Compassion	Honesty	Open minded	Team player
Charisma	Humanity	Open to correction	Understanding
Caring	Humor	Principled	Wisdom

### Appendix C – Murphy’s International Marketing Virtues

Virtue	Definition	Related Virtue
Integrity	Adherence to a moral code and completeness	Honesty, and Moral Courage
Fairness	Marked by equity and free from prejudice or favoritism	Justice
Trust	Faith or confidence in another party	Dependability
Respect	Giving regard to views of others	Consideration
Empathy	Being aware of and sensitive to the needs and concerns of others	Caring

### Appendix D – Blasi's Ordered Virtue Skills

Higher-Order Virtues	
Will Cluster	Integrity Cluster
Perseverance	Responsibility
Determination	Accountability
Self-discipline	Self-consistency
Self-control	Sincerity
Willpower	Integrity
	Principledness
	Transparency to oneself
	Honesty with oneself
	Autonomy
Lower-Ordered Virtues	
Empathy	Obedience
Compassion	Law-abidingness
Politeness	Civic-mindedness
Respectfulness	Honesty
Thoughtfulness	Conscientiousness
Kindness	Truthfulness
Generosity	Fairness
Altruism	Justice
Friendship	Courage
Loyalty	Humility

*Note:* Adapted from, Moral character: A psychological approach. In D. K. Lapsley & F. C. Power (Eds.), *Character psychology and character education* (p. 71 ). Notre Dame, IN: University of Notre Dame Press.

### Appendix E – Ethical Skills Required for Ethical Ability

Ethical Sensitivity	Ethical Judgment
Understanding emotional expression	Understanding ethical problems
Taking the perspectives of others	Using codes & identifying judgment criteria
Connecting to others	Reasoning critically
Responding to diversity	Reasoning ethically
Controlling social bias	Understanding consequences
Interpreting situations	Reflecting on process and outcome
Communicating well	Coping and resiliency

Ethical Focus	Ethical Action
Respecting others	Resolving conflicts and problems
Cultivating conscience	Asserting respectfully
Helping others	Taking initiative as a leader
Being a community member	Planning to implement decisions
Finding meaning in life	Cultivating courage
Valuing traditions & institutions	Persevering
Developing ethical identity & integrity	Working hard

*Note.* Adapted from, Narvaez, D. (2008). Human flourishing and moral development: Cognitive and neurobiological perspectives of virtue development. In L. P. Nucci & D. Narvaez (Eds.), *Handbook of Moral and Character Education* (pp. 310-327). New York, NY: Routledge.

## Appendix F – Four Processes, Their Skills, and Sub-skills

### Sensitivity

#### *ES – 1: Understand Emotional Expression*

Identify and express emotions  
 Fine-tune your emotions  
 Manage anger and aggression

#### *ES – 2: Take the Perspectives of Others*

Take an alternative perspective  
 Take a cultural perspective  
 Take a justice perspective

#### *ES – 3: Connecting to Others*

Relate to others  
 Show care  
 Be a friend

#### *ES – 4: Responding to diversity*

Work with group and individual differences  
 Perceive diversity  
 Become multicultural

#### *ES – 5: Controlling Social Bias*

Diagnose bias  
 Overcome bias  
 Nurture tolerance

#### *ES – 6: Interpreting Situations*

Determine what is happening  
 Perceive morality  
 Respond creatively

### Judgment

#### *EJ – 1: Understanding Ethical Problems*

Gathering information  
 Categorizing problems  
 Analyzing ethical problems

#### *EJ -2: Using Codes and Identifying Judgment Criteria*

Characterizing codes  
 Discerning code application  
 Judging code validity

#### *EJ – 3: Reasoning Generally*

Reasoning objectively  
 Using sound reasoning  
 Avoid reasoning pitfalls

#### *EJ – 4: Reasoning Ethically*

Judging perspectives  
 Reason about standards and ideals  
 Reason about actions and outcomes

#### *EJ – 5: Understand Consequences*

Analyzing consequences  
 Predicting consequences  
 Responding to consequences

#### *EJ – 6: Reflect on the Process and Outcome*

Reasoning about means and ends  
 Making right choices  
 Monitoring one's reasoning



## Appendix F – Four Processes, Their Skills, and Sub-skills (cont.)

### Sensitivity (cont.)

#### *ES – 7: Communicate Well*

Speak and listen  
 Communicate nonverbally and alternatively  
 Monitor communication

### Judgment (cont.)

#### *EJ – 7: Coping*

Apply positive reasoning  
 Managing disappointment and failure  
 Developing resilience

### Motivation

#### *EM – 1: Respecting Others*

Be civil and courteous  
 Be non-violent  
 Show reverence

#### *EM – 2: Cultivate Conscience*

Self-command  
 Manage influence and power  
 Be honorable

#### *EM – 3: Act Responsibly*

Meet obligations  
 Be a good steward  
 Be a global citizen

#### *EM – 4: Help Others*

Cooperate  
 Act thoughtfully  
 Share resources

#### *EM – 5: Finding Meaning in Life*

Center yourself  
 Cultivate commitment  
 Cultivate wonder

### Action

#### *EA – 1: Resolving Conflicts and Problems*

Solve interpersonal problems  
 Negotiate  
 Make amends

#### *EA – 2: Assert Respectfully*

Attend to human needs  
 Build assertiveness skills  
 Use rhetoric respectfully

#### *EA – 3: Taking Initiative as a Leader*

Be a leader  
 Take initiative for and with others  
 Mentor others

#### *EA – 4: Planning to Implement Decisions*

Thinking strategically  
 Implement successfully  
 Determine resource use

#### *EA – 5: Cultivate Change*

Manage fear  
 Stand up under pressure  
 Managing change and uncertainty

## Appendix F – Four Processes, Their Skills, and Sub-skills (cont.)

### Motivation (cont.)

#### *EM – 6: Valuing Traditions and Institutions*

Identify and value traditions

Understand social structures

Practice democracy

#### *EM – 7: Develop Ethical Identity and Integrity*

Choose good values

Build your identity

Reach for your potential

### Action (cont.)

#### *EM – 6: Persevering*

Be steadfast

Overcome obstacles

Build competence

#### *EA – 7: Work Hard*

Set reachable goals

Manage time

Take charge of your life

## Appendix G – Attributes of Professionalism in Computing

- The professional has a sense of responsibility for the quality of the work performed, a high self-imposed standard of workmanship to maintain that quality, and joy and pride in performing that work
- A willingness to attempt to understand and think like the users, customers or consumers of the products they are developing
- Existence of an accepted commitment or calling or sense of responsibility for serving the public
- The professional has a high degree of individual responsibility, a willingness to take initiatives, and a sense of obligation to identify client (and employer) needs as well as client (and employer) wants
- Thinks creatively
- Logical reasoning
- Application of skills based on special knowledge
- Know and respect laws pertaining to the professional work
- Demonstrates loyalty
- Honesty, trustworthiness, avoid hurting others
- The professional is aware of the effects that services performed have on society and has a sense of responsibility for serving the public good
- The professional has an understanding of the interaction and relationship between facts and values (or technology and values
- Being willing to put in the extra effort needed to successfully complete necessary tasks
- Acquire and maintain professional competence
- Advanced education and training
- Existence of a code of conduct or ethics
- Shows a personal commitment to quality
- Meets client/user expectations
- Is a team player
- Is open to constructive critiques on how to improve

---

*Note.* Adapted from Fuller, U., Keim, B., Fitch, D., Little, J. C., Riedesel, C., & White, S. (2009). Perspectives on developing and accessing professional values in computing. *ACM SIG on Computer Science Education*, 41(4), 174-194.

## Appendix H – Four-Component Model of Moral Action in Computing

Moral imagination. Projecting oneself into the perspective of others

**Skills** Constructing the relevant stakeholders in a socio-technical system; data collection about stakeholders; understanding stakeholder perspectives

**Knowledge** Specific knowledge about the domain (e.g. privacy, safety, equity); knowledge of socio-technical systems; knowledge of methods to investigate stakeholder perspectives

Moral creativity. Generating solutions to moral challenges while responding to multiple constraints

**Skills** Identifying value conflicts in a socio-technical system; constructing and evaluating solutions under constraint

**Knowledge** Specific knowledge about domains (e.g. privacy, safety, equity); technical knowledge of constraints and opportunities; knowledge of socio-technical systems

Reasonableness. Engaging in reasoned dialogue with openness

**Skills** Constructing data-based and reasoned arguments; engaging in reasoned dialogue, gathering relevant evidence, listening to others, giving reasons, changing plans/positions based on reason

**Knowledge** Specific knowledge about domain (e.g. privacy, safety, equity); technical knowledge of constraints and opportunities; knowledge of ethical argumentation

## Appendix H – Four-Component Model of Moral Action in Computing

Perseverance. Planning moral action and responding to unforeseen circumstances while keeping moral goals intact

Skills	Constructing and revising implementation plans based on organizational constraints. Negotiation within complex organizational environments
Knowledge	Specific knowledge about domain (e.g. privacy, safety, equity); knowledge of socio-technical systems; knowledge of ethical dissent and whistleblowing

**Appendix I – SMEs PPSS**

1. Education: (please select the highest degree attained, if both a JD and Ph.D. select both)

Bachelor's Degree

Master's Degree

Doctoral Degree

Juris Doctorate

2. Specialized Industry Certifications: (such as CISSP, IAAP, SSCP, GIAC, CISM, CEH, CSFA)

A. \_\_\_\_\_

B. \_\_\_\_\_

C. \_\_\_\_\_

D. \_\_\_\_\_

E. \_\_\_\_\_

3. Occupation:

Computer Ethicist/Philosopher Professor

IS/IT Professor

Law Professor (specialist in information privacy and or security)

Chief Information Officer (CIO)

Chief Privacy Officer (CPO)

Security or Privacy Specialist

Other \_\_\_\_\_

**Appendix I – SMEs PPSS (cont.)**

## 4. Years at Current Occupation:

 3 – 5 Years 6 – 10 Years 11 – 15 Years 16+ Years

### Appendix I – SMEs PPSS (cont.)

1. A fellow IS/IT colleague who is a close friend is out of the office for a week. You left your biometric personal identity information badge at home and need to get into a secure area of the building that your friend also accesses. Your friend left his badge in his desk, and has told you in the past if you need to use his badge to get it out of his desk drawer and use it. You allow him to do the same with your badge. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

2. A different IS/IT employee is out of the office for a week who is not a close friend. You left your biometric personal identity information badge at home and need to get into a secure area of the building that this person can access. Their badge is in their desk, so you (i.e, the employee) decide to borrow the badge. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	



**Appendix I – SMEs PPSS (cont.)**

3. You are the director of IS/IT at a company. You suspect one of your employees of unethical behaviors that have to do with emails, so after hours you read the employee's emails so that you have supporting evidence when you go to human resources with the problem. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

4. You are a database engineer who works for one of the three major credit card verification bureaus. A friend moved out of town without giving you a forward address or telephone number, and this person owes you \$10,000. You decide to use your company's database to locate this person and try to get your money back. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

5. You are an IT supervisor at the university that your child attends. You suspect that the money that you are giving your child to pay for classes is being spent on things other than classes, so you log into your child's student account to determine if in fact they have been registering for classes. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

6. A new technology management position will be opening in 6 months with a salary that is \$12,000 over your current salary. You and your spouse desperately need a new vehicle. You have access to the human resources databases. You open the human resources database to examine your co-workers resumes so that you could gain a competitive advantage and get the job. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

7. You are a database administrator. Your company has one of the largest national marketing databases that contain approximately 95% of U.S. citizens' whereabouts, with home and cell telephone numbers, current address, current employer, drivers' license numbers, and Social Security Numbers. You had a close friend from high school and college that you have not seen or spoken with in sometime, and you would like to invite them to your wedding. Since obtaining the information would not hurt anyone, you access your company's database to retrieve your friends contact information. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

8. You use your network administrators' password to gain access to the human resources server, and remove any negative reviews about your job performance that could put your job in jeopardy or prevent you from getting a raise in pay. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

9. The company you work for is downsizing the IT department you work in. One more employee will be fired, and it is between you and someone else. You found out that the other employee has AIDS by looking through their personal emails at the office. Would you inform your supervisor of this if you knew it would save your job and you did not have to let anyone know how you actually obtained the information? Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

10. You are an IS/IT employee on your lunch-break. Your job gives you access to all the company email. Just playing around, and not intending to do any harm you pass time by reading internal company emails. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

### Appendix I – SMEs PPSS (cont.)

11. You work in your local hospitals IS/IT department and have access to all the computer systems throughout the hospital. You found out from one of your neighbors that another neighbor is sick and in the hospital, so you log into the patient records system to find out what your neighbor's ailment is and what room they are in so you can go and visit them. Do you believe that this is an unethical privacy violation?

Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

12. You work in the IS/IT department for American Express as one of the senior system administrators, you have access to all card member information. A friend is overdue with his payment because he lost his job, so you go into the customer database and remove any charges on the credit card. You believe that this is no big deal because American Express is a huge international corporation that will not miss the money, and there is no way that you could get caught since you are in charge of all of the audit tracking software on the network. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

13. You know that you are going to be fired from your job. So you to take logins, passwords, and marketing information of company clients to gain a competitive advantage for a new employer. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

14. A fellow employee that you have been interested in for some time asks you out. You tell them that you are interested in them also but are busy this weekend. You tell them this so that you can do a background check on them to make sure that there is nothing questionable in their past. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

15. You and your spouse work for the same company, you in the IS/IT department and your wife in the accounting department. You suspect that the head of the accounting department and your spouse are having an affair. You log into both of their office emails and your spouse's personal email outside of the office to see if you can determine anything. Do you believe that this is an unethical privacy violation?

Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

16. You work in your company's IS/IT department. While walking down a hall one day, you notice one of the company cell phones that all of the executives carry, and it is on the floor. Rather than giving it to the security officer of the IS/IT department you logon to it and bring up the person information so that you can give the cell phone back to the correct person. Do you believe that this is an unethical privacy violation?

Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

17. You work in the IS/IT department of the state's department of transportation. Your friend's car failed its safety and emissions test, and therefore did not get its safety certification. This means their auto insurance will be canceled because they cannot afford the \$1,500.00 to repair the car. Rather than let them lose their insurance, you change the database information that contains all of your friends pertinent and personal information to show that the car passed inspection and you give your friend a window decal signifying that it passed its annual inspection. Your reasoning is that no one is getting hurt and you are helping a friend. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

18. You work in your university's IS/IT department. The university is withholding your sister's diploma due to a late fee on a library book that you know she never checked out. So you access your sister's school records to erase the fine so that she can graduate, especially since the action would not hurt anyone. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	



**Appendix I – SMEs PPSS (cont.)**

19. You have been told that when you finish your master's degree in management and information systems you will be given an assistant director's position within the IS/IT department. Your database course has a capstone project due at the end of the semester. The project is to put together a database with consumer's marketing information that identifies individuals by name, email address, their zip code, and other personal information. Since you are not sure how to do this, you ask your friend who is one of the company's database programmers to help you compile the information using data from the company that you work for so you can turn it in as part of your capstone project. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

20. Your boss, the head of the IT department is no nonsense dictator who really pushes everyone to work hard. For his birthday you get him a really nice pen that you know he will always use that has a small RFID tracking device in it so you know where he always is; this way you and the IT team can take it easy when he is not around. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

21. You are the director of all IS/IT services at the same university that your spouse is the chair of the English department. Your spouse calls you and tells you that she has misplaced some personal information for a few professors whose information must go on a federal grant that the English department is applying for, and that the grant must be submitted by the end of the day. You know that she has had all of the professor's identification numbers, Social Security Numbers, and other germane information that she needs to finish the grant. Knowing that she previously had all of this personal information for the professors you log into the appropriate server to get here the information again, even though the university has a protocol for requesting this type of information that is supposed to go through the university's grant writing office. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

22. You work in the IS/IT department for major pharmacy/drug store chain. Your best friend is sick and ran-out of prescription refills. It is Saturday morning and your friend cannot get back to the doctors before Monday. You go into the patient/customer database and put a checkmark next to “allow one more refill.” Since you are the only one that controls the database auditing for prescriptions no one will know you did this. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

23. You believe that you are being paid less than your peers with the same educational and job experience, so you access the payroll records on the accounting and human resources server to enquire. You do this because you know that you will be able to use the information when it comes time for a pay raise. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

24. The company that you work for is publically traded on the New York Stock Exchange. You are responsible for all of you company's email servers. You have information that would indicate that the company that you work for is probably going to be bought-out by a larger competitor, thereby making your company's stock more than quadruple. Owning over five thousand shares of stock at \$10.00 a share you want to determine if this buy-out is true so that you can invest more of your money in your company. Knowing that if you invest more money it will not hurt anyone, you run an email scan of all the company's board members to determine if the information is true. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

25. You know that your job might be at risk, so you to take the pre-emptive move of downloading your company's sensitive and private information to help you gain a competitive advantage at securing a new position with a different company. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

26. You work at a nearby hospital as a network engineer, and are taking databases courses at night. One day on your lunch break, you begin practicing your data mining and extraction skills by developing a query that extracts information for patients who were admitted to the hospital over the past year. You tell the query to include patient name, SSN#, gender, date of admission, home address, phone number, health insurance provider... However, since this information will never be used for anything, and you are the only one that will ever see the information, you assume it is fine to practice your new skills this way. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

27. You know that an employee at the company you work for keeps explicit pictures of his wife who is a nude model on his computer's hard drive. As an IS/IT administrator you have access to all the company's computers. You log onto this employees PC remotely and look at the pictures since other IS/IT administrators have done so too. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

28. You are the director of the IS/IT department and your spouse is the director of the grant-writing department at a large hospital and medical research center. Your spouse calls you one day and tells you that she does not have the time to chase down five specific doctors who work for the hospital to get some pieces of personally identifiable information that are required for a 20 million dollar research grant from the National Institute of Health. The electronic submission deadline for the grant request is 3:00 pm the day she calls you and it is already 1:30 pm. Hospital policy states that this type of information must come from the human resources department, but the human resources department told your wife that they could not get her the information until the next day. Knowing that you have access to the human resources databases, and that the grant is very important to the hospital, you merge data from different databases to get her the physician's state license numbers, SSN's, board certification numbers, hospital office numbers and telephone numbers, and home addresses and telephone numbers.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

29. You are one of this country's brightest network security people. Many of your skills were self-taught by learning to hack networks. The police arrested the two individuals that abducted and molested your 17 year old daughter two weeks ago; thankfully she is home and safe now. During the criminal's trial, it was brought out that they were frequent subscribers to adult pornographic websites. Ironically, more and more of these so-called pornographic abductions have begun to take place across the country. To help combat this type of crime, and raise the awareness of parents all over the country, you hack into some of the most major and offensive pornographic websites and then leak the names of users over the Internet. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6	
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical		

30. You work in the IS/IT department of a large marketing firm and have access to a huge consumer database that contains information like addresses and emails. You are in your last year of college and money is running tight. Since it will not hurt anyone, you access to corporate database of customers so you can send out emails requesting society's help to get you through college. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6	
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical		

### Appendix I – SMEs PPSS (cont.)

31. You are a network and applications engineer for an organization. While working on the laptop of the director of finance you notice that the laptop contained hundreds of underage pornographic pictures. Knowing that child pornography is illegal, you scan the directors emails to determine if any attachments can be found indicating where these pictures came from, and to determine if the director of finance is doing anything else illegal before reporting this activity to your boss and the authorities. Do you believe that this is an unethical privacy violation? Please select one response from below. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation		Minimally Unethical		Moderately Unethical		Highly Unethical

32. Your parents, spouse, and two children were killed in a car crash by someone authorized to use marijuana by the Medical Marijuana Access Program that is sponsored the government. This is not the first of these types of accidents in the country, but this time the government's program has taken your family members from you. In retaliation, you leak over the Internet the entire database of patient's names who receive medical marijuana. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation		Minimally Unethical		Moderately Unethical		Highly Unethical



**Appendix I – SMEs PPSS (cont.)**

33. You work for a mobile phone company and saw an advertisement in a newspaper about a car for sale. The car sounded like a good buy. The advertisement listed the seller's mobile phone number, but not the seller's address. Being a system software engineer for the mobile phone company you knew that you could determine the seller's address by accessing the seller's mobile phone records, which you did and went to the seller's house to discuss buying the car. The seller was delighted and the sale went through. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

34. Being the good IS/IT practitioner that you are, during your lunch break you search your company's network for security holes. You come across a hole that exposes some form of personally identifiable information for every employee in the company. To determine the severity of the hole, you set out to find exactly what information is being exposed for each of the company's employees even though your boss did not ask you to do this. Your reasoning is to help protect privacy, and look good to your boss when promotion time comes around. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

35. You are a programmer for a mid-sized company that is downsizing the IT department you work in. One more employee will be let go, and it is between you and someone else. You know how to inject code into the other employees programming that would cause their program to malfunction and expose personally identifiable information of the company's clients. You cannot afford to lose your job because your daughter's health is very fragile and she requires specialized medications that you cannot afford without your company's health insurance plan. So you inject the code. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

36. You work in your local hospitals IS/IT department on patient files. Your father has been in and out of the hospital's emergency room a number of times over the past few months, but when you question him, he says it is no big deal. Your mother passed away last year and both you and your older sister are concerned for your father's health so you log into his patient file to determine his health status. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

### Appendix I – SMEs PPSS (cont.)

37. You are the only female network engineer among three other male network engineers for a mid-sized company. While working late one night, you notice that your boss has left his computer on. You enter his office to turn off the monitor and find that his email is still open. You notice that one of the email headers is about you so you open the email only to find out that your boss and other male network engineers have been discussing you behind your back in sexually explicit manner. You print out the emails and bring them to the head of human resources the very next day. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

38. You are a IS/IT data analyst at a major casino working after normal business hours to finish an important project that is due the next day. You realize that you are missing data that was originally sent to you by a fellow IS/IT coworker. You inadvertently observed your coworker typing their password several days ago, so you decide to login into the system as them and resend the data to yourself so that you can complete the project. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

**Appendix I – SMEs PPSS (cont.)**

39. You are the chief database architect for the world's largest commercial database on consumers. In essence, you have absolute control over all data. The database contains information on over 500 million active consumers worldwide, and it processes over 2,000 data points' per person each year. Covertly covering your tracks, you leak the entire database to a number of huge companies. For these actions, you are paid nearly 700 million dollars. For legal protection, you immediately leave this country for a country with no extradition treaty with the U.S. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

40. You log into a university student database to change a coworker's grade from a B+ to an A, because without an A in a particular computer security course your friend will be terminated from his current job. Do you believe that this is an unethical privacy violation? Please select one response from below.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	2	3	4	5	6
No Violation	Minimally Unethical		Moderately Unethical		Highly Unethical	

### **Appendix J – SMEs Invitation to Participate Email**

My name is Mark Rosenbaum. I am currently a doctoral candidate working on my dissertation in the Graduate School of Computer and Information Sciences at Nova Southeastern University in Florida. As a subject matter expert in privacy and information systems and information technology, I am requesting your participation with my dissertation research to help establish a reliability and validation criteria for a new Personally Identifiable Information (PII) privacy violations scale based on the severity of privacy violation. The results of this survey will aid in creating an IS/IT privacy violations scale that can then be administered to working IS/IT practitioners to determine how likely they are to commit some of the violations that you will be interpreting. I believe that you have the skills and experience that would contribute greatly to the development of this assessment instrument. The survey instrument that I am requesting your participation with contains 40 scenarios related to privacy violations to PII. I anticipate that it will take approximately 15 minutes to complete the survey. I would greatly appreciate your participation. If interested in helping me establish this new privacy survey, and completing my dissertation research, please follow the link below to the survey. If you have any questions or concerns, please feel free to contact me.

[Survey Link Removed]

Thank you,

Mark H. Rosenbaum  
[mrosenba@nova.edu](mailto:mrosenba@nova.edu)  
(305) 666-0505

Dr. Ling Wang  
Dissertation Chair  
[lingwang@nova.edu](mailto:lingwang@nova.edu)  
(954) 262-2020

## **Appendix K – Introduction to PPSS Survey for SMEs**

As a subject matter expert in privacy and information systems and information technology, you have been selected to participate in the development of a new Personally Identifiable Information (PII) privacy violations scale that is based on the severity of privacy violations. The results of this survey will aid in creating an IS/IT privacy violations scale that can then be administered to working IS/IT practitioners to determine how likely they are to commit some of the violations that you will be interpreting. After reading the instructions below you will be presented with some general demographic questions and then the 40 PII privacy violation scenarios. The total time to complete the survey is about 15 minutes. However, due to the length of the survey and as a convenience to you, the survey has a STOP and CONTINUE function after each 10 privacy violation questions. If you choose to temporarily stop and close your browser window after completing any page, you can re-click the link in your email and you will be taken back to where you left off on the survey. Additionally, while your name and email address in LinkedIn was used to contact you, none of your data responses will specifically link you the results of your survey participation. Your cooperation in fully completing this survey is greatly appreciated.

Mark H. Rosenbaum  
[mrosenba@nova.edu](mailto:mrosenba@nova.edu)  
(305) 666-0505

Dr. Ling Wang  
Dissertation Chair  
[lingwang@nova.edu](mailto:lingwang@nova.edu)  
(954) 262-2020

### **Appendix L – Introduction and Instruction Letter to SMEs for PPSS Survey**

Please refer to the following sections of part a), part b), and part c) below for instructions on completing the survey and the operationalization of terms.

a) There is a Likert scale below each of the PII privacy violation. The scale goes from zero (0) to six (6). The number zero (0) represents “no violation” in privacy to PII, while the numbers of 1 through 6 represent gradations of minimally unethical to highly unethical privacy violations. Your task is to rate the scenarios in terms of how unethical you think each one is, that is to say you are interpreting each scenario as if it were a behavior done by a person. Please select the numbered box below each of the scenarios that you believe to be most appropriate.

b) Interpret the behavioral scenarios as if you were assessing someone’s behavior. When interpreting the behaviors in the scenarios, please consider the following: The scenarios differ on a variety of dimensions, including things like intention, amount of harm, type of harm (e.g., psychological, financial, legal, physical, social...), mitigating circumstances, and rationale given by the actor. There are extensive literatures associated with each of these dimensions, and psychologists, computer ethicists, and lawmakers at times disagree on which dimensions are relevant or most important. Please use your own judgment in deciding if these things influence your ratings for how unethical you think each of these privacy violations to personally identifiable information is. To construct the final scale, I will be averaging your ratings with those of other experts and choosing those scenarios that have the most consensus and that provide a range of scores on the ratings. Therefore, what I am requesting of you is your best guess about how unethical each of the given scenarios/actions is, given the limited information in each scenario.

c) There is a comment box at the end of the survey for remarks. Please feel free to

**Appendix L – Introduction and Instruction Letter to SMEs for PPSS Survey (cont.)**

provide any commentary that you believe would be useful in the development of this instrument.

d) Below the comment box is space for you to recommend colleagues names and email addresses for participation in this survey, should you choose to do so. Again, thank you for your time and assistance.

Mark H. Rosenbaum  
[mrosenba@nova.edu](mailto:mrosenba@nova.edu)  
(305) 666-0505

Dr. Ling Wang  
Dissertation Chair  
[lingwang@nova.edu](mailto:lingwang@nova.edu)  
(954) 262-2020



### Appendix M – SMEs Demographics

Item	Frequency	Percentage
<i>Education</i>		
Bachelor's Degree	11	20.75%
Master's Degree	15	28.13%
Ph.D.	19	35.84%
J.D.	5	9.43%
Master's Degree & J.D.	2	3.77%
Ph.D. & J.D.	1	1.88%
<i>Occupation</i>		
Chief Information Officer	1	1.88%
Computer Ethicist (Professor)	5	9.43%
Chief Privacy Officer	15	28.30%
IS/IT Professor	14	26.41%
Philosophy Professor	4	7.54%
Privacy Law Professor	1	1.88%
Psychologist Privacy Professor	1	1.88%
Security/Privacy Specialist	28	52.83%
<i>Years at Present Occupation</i>		
10 years	6	11.32%
11 -15 years	20	37.73%
16+ years	27	50.94%

**Appendix M – SMEs Demographic Data (cont.)**

Item	Frequency	Percentage
<i>Country</i>		
Australia	1	1.88%
France	1	1.88%
India	1	1.88%
Japan	1	1.88%
Taiwan	1	1.88%
United Kingdom	1	1.88%
United States	47	88.67%
<i>Industry Certifications</i>		
Certified Information Privacy Professional – CIPP	30	56.60%
Certified Information Systems Security Professional – CISSP	11	20.75%
Certified Information Security Manger – CISM	8	15.09%
Certified Information Systems Auditor – CISA	5	9.43%
Info. Technology Infrastructure Library Certification – ITIL	4	7.54%
Certified Information Privacy Manager – CIPM	3	5.66%
Certificate of Cloud Security Knowledge – CCSK	2	3.77%
Certified Ethical Hacker – CEH	2	3.77%
Certification in the Governance of Enterprise IT – CGEIT	2	3.77%
Certified Information Privacy Technologist – CIPT	2	3.77%
Info. Systems Security Management Professional – ISSMP	2	3.77%
Project Management Professional Certification – PMP	2	3.77%

**Appendix M – SMEs Demographic Data (cont.)**

Item	Frequency	Percentage
Associate Business Continuity Professional – ABCP	1	1.88%
Access Data Certified Examiner – ACE	1	1.88%
Business Continuity Certified Specialist – BCCS	1	1.88%
Certified Chief Information Officer – C CISO	1	1.88%
California Attorney	1	1.88%
Certified Check Point Security Administrator – CCSA	1	1.88%
Certified Data Processor – CDP	1	1.88%
Certificate in Information Assurance & Cybersecurity	1	1.88%
Certified Information Security Auditor – CISA	1	1.88%
Certified Healthcare Chief Information Officer – CHCIO	1	1.88%
Certified Payment-Card Industry Security Manager – CPISI	1	1.88%
Certified in Risk and Information Systems Control – CRISC	1	1.88%
EC-Council Certified Security Analyst – ECSA	1	1.88%
EMC Cloud Architect – EMCCA	1	1.88%
Global Certified Forensic Analyst – GCFA	1	1.88%
Healthcare Info. Security Privacy Professional – HCISPP	1	1.88%
ISO 27001:2013 Lead Auditor	1	1.88%
Info. Systems Security Architecture Professional – ISSAP	1	1.88%
Payment Card Ind.-Qualified Security Assessor – PCI-QSA	1	1.88%
Professional Engineer – PE	1	1.88%
Security+	1	1.88%

**Appendix N – SMEs PPSS Measures of Central Tendency**

Question Number	Mean	Standard Deviation	Variance
1	3.04	2.075	4.306
2	5.00	1.240	1.538
3	3.19	2.458	6.041
4	5.40	1.062	1.128
5	4.51	1.694	2.870
6	5.85	.411	.169
7	4.98	1.366	1.865
8	5.43	1.635	2.673
9	5.85	.456	.208
10	5.70	.540	.292
11	5.47	.953	.908
12	5.58	1.184	1.401
13	5.68	.976	.953
14	1.66	2.166	4.690
15	5.55	1.030	1.060
16	3.19	1.971	3.887
17	5.38	1.390	1.932
18	4.89	1.750	3.064
19	4.91	1.713	2.933
20	5.51	.973	.947
21	4.15	1.791	3.208
22	5.26	1.546	2.390

**Appendix N – SMEs PPSS Measures of Central Tendency (cont.)**

Question Number	Mean	Standard Deviation	Variance
23	5.62	1.096	1.201
24	5.74	.655	.429
25	4.94	1.703	2.901
26	4.57	1.658	2.750
27	5.77	.724	.525
28	5.25	1.413	1.996
29	3.87	2.219	4.925
30	4.83	1.464	2.144
31	5.62	1.023	1.047
32	3.43	2.043	4.173
33	5.70	.638	.407
34	5.70	.799	.638
35	4.21	1.680	2.821
36	4.75	1.343	1.804
37	5.85	.533	.284
38	5.06	1.365	1.862
39	5.89	.506	.256
40	5.36	1.331	1.773

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
1	3.04	2.075	4.306	A fellow IS/IT colleague who is a close friend is out of the office for a week. You left your biometric personal identity information badge at home and need to get into a secure area of the building that your friend also accesses. Your friend left his badge in his desk, and has told you in the past if you need to use his badge to get it out of his desk drawer and use it. You allow him to do the same with your badge. Do you believe that this is an unethical privacy violation? Please select one response from below.	.930
2	5.00	1.240	1.538	A different IS/IT employee is out of the office for a week who is not a close friend. You left your biometric personal identity information badge at home and need to get into a secure area of the building that this person can access. Their badge is in their desk, so you (i.e., the employee) decide to borrow the badge. Do you believe that this is an unethical privacy violation? Please select one response from below.	.931

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
3	3.19	2.458	6.041	You are the director of IS/IT at a company. You suspect one of your employees of unethical behaviors that have to do with emails, so after hours you read the employee's emails so that you have supporting evidence when you go to human resources with the problem. Do you believe that this is an unethical privacy violation? Please select one response from below.	.937
4	5.40	1.062	1.128	You are a database engineer who works for one of the three major credit card verification bureaus. A friend moved out of town without giving you a forward address or telephone number, and this person owes you \$10,000. You decide to use your company's database to locate this person and try to get your money back. Do you believe that this is an unethical privacy violation? Please select one response from below.	.930

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
5	4.51	1.694	2.870	You are an IT supervisor at the university that your child attends. You suspect that the money that you are giving your child to pay for classes is being spent on things other than classes, so you log into your child's student account to determine if in fact they have been registering for classes. Do you believe that this is an unethical privacy violation? Please select one response from below.	.931
6	5.85	.411	.169	A new technology management position will be opening in 6 months with a salary that is \$12,000 over your current salary. You and your spouse desperately need a new vehicle. You have access to the human resources databases. You open the human resources database to examine your co-workers resumes so that you could gain a competitive advantage and get the job. Do you believe that this is an unethical privacy violation? Please select one response from below.	.931



**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
7	4.98	1.366	1.865	You are a database administrator. Your company has one of the largest national marketing databases that contain approximately 95% of U.S. citizens' whereabouts, with home and cell telephone numbers, current address, current employer, drivers' license numbers, and Social Security Numbers. You had a close friend from high school and college that you have not seen or spoken with in sometime, and you would like to invite them to your wedding. Since obtaining the information would not hurt anyone, you access your company's database to retrieve your friends contact information. Do you believe that this is an unethical privacy violation? Please select one response from below.	.930

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
8	5.43	1.635	2.673	You use your network administrators password to gain access to the human resources server, and remove any negative reviews about your job performance that could put your job in jeopardy or prevent you from getting a raise in pay Do you believe that this is an unethical privacy violation? Please select one response from below.	.930
9	5.85	.456	.208	The company you work for is downsizing the IT department you work in. One more employee will be fired, and it is between you and someone else. You found out that the other employee has AIDS by looking through their personal emails at the office. Would you inform your supervisor of this if you knew it would save your job and you did not have to let anyone know how you actually obtained the information? Do you believe that this is an unethical privacy violation? Please select one response from below.	.931

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
10	5.70	.540	.292	You are an IS/IT employee on your lunch-break. Your job gives you access to all the company email. Just playing around, and not intending to do any harm you pass time by reading internal company emails. Do you believe that this is an unethical privacy violation? Please select one response from below.	.931
11	5.47	.953	.908	You work in your local hospitals IS/IT department and have access to all the computer systems throughout the hospital. You found out from one of your neighbors that another neighbor is sick and in the hospital, so you log into the patient records system to find out what your neighbor's ailment is and what room they are in so you can go and visit them. Do you believe that this is an unethical privacy violation? Please select one response from below.	.930

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
12	5.58	1.184	1.401	You work in the IS/IT department for American Express as one of the senior system administrators, you have access to all card member information. A friend is overdue with his payment because he lost his job, so you go into the customer database and remove any charges on the credit card. You believe that this is no big deal because American Express is a huge international corporation that will not miss the money, and there is no way that you could get caught since you are in charge of all of the audit tracking software on the network. Do you believe that this is an unethical privacy violation? Please select one response from below.	.929
13	5.68	.976	.953	You know that you are going to be fired from your job. So you to take logins, passwords, and marketing information of company clients to gain a competitive advantage for a new employer. Do you believe that this is an unethical privacy violation? Please select one response from below.	.930

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
14	1.66	2.166	4.690	A fellow employee that you have been interested in for some time asks you out. You tell them that you are interested in them also but are busy this weekend. You tell them this so that you can do a background check on them to make sure that there is nothing questionable in their past. Do you believe that this is an unethical privacy violation? Please select one response from below.	.936
15	5.55	1.030	1.060	You and your spouse work for the same company, you in the IS/IT department and your wife in the accounting department. You suspect that the head of the accounting department and your spouse are having an affair. You log into both of their office emails and your spouse's personal email outside of the office to see if you can determine anything. Do you believe that this is an unethical privacy violation? Please select one response from below.	.929

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
16	3.19	1.971	3.887	You work in your company's IS/IT department. While walking down a hall one day, you notice one of the company cell phones that all of the executives carry, and it is on the floor. Rather than giving it to the security officer of the IS/IT department you logon to it and bring up the person information so that you can give the cell phone back to the correct person. Do you believe that this is an unethical privacy violation? Please select one response from below.	.930

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
17	5.38	1.390	1.932	You work in the IS/IT department of the state's department of transportation. Your friend's car failed its safety and emissions test, and therefore did not get its safety certification. This means their auto insurance will be canceled because they cannot afford the \$1,500.00 to repair the car. Rather than let them lose their insurance, you change the database information that contains all of your friends pertinent and personal information to show that the car passed inspection and you give your friend a window decal signifying that it passed its annual inspection. Your reasoning is that no one is getting hurt and you are helping a friend. Do you believe that this is an unethical privacy violation? Please select one response from below.	.929

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
18	4.89	1.750	3.064	You work in your university's IS/IT department. The university is withholding your sister's diploma due to a late fee on a library book that you know she never checked out. So you access your sister's school records to erase the fine so that she can graduate, especially since the action would not hurt anyone. Do you believe that this is an unethical privacy violation? Please select one response from below.	.927



**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
19	4.91	1.713	2.933	You have been told that when you finish your master's degree in management and information systems you will be given an assistant director's position within the IS/IT department. Your database course has a capstone project due at the end of the semester. The project is to put together a database with consumer's marketing information that identifies individuals by name, email address, their zip code, and other personal information. Since you are not sure how to do this, you ask your friend who is one of the company's database programmers to help you compile the information using data from the company that you work for so you can turn it in as part of your capstone project. Do you believe that this is an unethical privacy violation? Please select one response from below.	.931

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
20	5.51	.973	.947	Your boss, the head of the IT department is no nonsense dictator who really pushes everyone to work hard. For his birthday you get him a really nice pen that you know he will always use that has a small RFID tracking device in it so you know where he always is; this way you and the IT team can take it easy when he is not around. Do you believe that this is an unethical privacy violation? Please select one response from below.	.930

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
21	4.15	1.791	3.208	You are the director of all IS/IT services at the same university that your spouse is the chair of the English department. Your spouse calls you and tells you that she has misplaced some personal information for a few professors whose information must go on a federal grant that the English department is applying for, and that the grant must be submitted by the end of the day. You know that she has had all of the professor's identification numbers, Social Security Numbers, and other germane information that she needs to finish the grant. Knowing that she previously had all of this personal information for the professors you log into the appropriate server to get here the information again, even though the university has a protocol for requesting this type of information that is supposed to go through the university's grant writing office. Do you believe that this is an unethical privacy violation? Please select one response from below.	.927

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
22	5.26	1.546	2.390	<p>You work in the IS/IT department for major pharmacy/drug store chain.</p> <p>Your best friend is sick and ran-out of prescription refills. It is Saturday morning and your friend cannot get back to the doctors before Monday.</p> <p>You go into the patient/customer database and put a checkmark next to “allow one more refill.” Since you are the only one that controls the database auditing for prescriptions no one will know you did this. Do you believe that this is an unethical privacy violation? Please select one response from below.</p>	.929
23	5.62	1.096	1.201	<p>You believe that you are being paid less than your peers with the same educational and job experience, so you access the payroll records on the accounting and human resources server to enquire. You do this because you know that you will be able to use the information when it comes time for a pay raise. Do you believe that this is an unethical privacy violation? Please select one response from below.</p>	.930

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
24	5.74	.655	.429	The company that you work for is publically traded on the New York Stock Exchange. You are responsible for all of you company's email servers. You have information that would indicate that the company that you work for is probably going to be bought-out by a larger competitor, thereby making your company's stock more than quadruple. Owning over five thousand shares of stock at \$10.00 a share you want to determine if this buy-out is true so that you can invest more of your money in your company. Knowing that if you invest more money it will not hurt anyone, you run an email scan of all the company's board members to determine if the information is true. Do you believe that this is an unethical privacy violation? Please select one response from below.	.930

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
25	4.94	1.703	2.901	You know that your job might be at risk, so you to take the pre-emptive move of downloading your company's sensitive and private information to help you gain a competitive advantage at securing a new position with a different company. Do you believe that this is an unethical privacy violation? Please select one response from below.	.928

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
26	4.57	1.658	2.750	<p>You work at a nearby hospital as a network engineer, and are taking databases courses at night. One day on your lunch break, you begin practicing your data mining and extraction skills by developing a query that extracts information for patients who were admitted to the hospital over the past year. You tell the query to include patient name, SSN#, gender, date of admission, home address, phone number, health insurance provider...</p> <p>However, since this information will never be used for anything, and you are the only one that will ever see the information, you assume it is fine to practice your new skills this way. Do you believe that this is an unethical privacy violation? Please select one response from below.</p>	.927

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
27	5.77	.724	.525	You know that an employee at the company you work for keeps explicit pictures of his wife who is a nude model on his computer's hard drive. As an IS/IT administrator you have access to all the company's computers. You log onto this employees PC remotely and look at the pictures since other IS/IT administrators have done so too. Do you believe that this is an unethical privacy violation? Please select one response from below.	.931



**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
28	5.25	1.413	1.996	You are the director of the IS/IT department and your spouse is the director of the grant-writing department at a large hospital and medical research center. Your spouse calls you one day and tells you that she does not have the time to chase down five specific doctors who work for the hospital to get some pieces of personally identifiable information that are required for a 20 million dollar research grant from the National Institute of Health. The electronic submission deadline for the grant request is 3:00 pm the day she calls you and it is already 1:30 pm. Hospital policy states that this type of information must come from the human resources department, but the human resources department told your wife that they could not get her the information until the next day. Knowing that you have access to the human resources databases, and that the grant is very important to the hospital, you merge data from different databases to get her the physician's state license numbers, SSN's, board certification numbers, hospital office numbers and telephone numbers, and home addresses and telephone numbers.	.930

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
29	3.87	2.219	4.925	<p>You are one of this country's brightest network security people. Many of your skills were self-taught by learning to hack networks. The police arrested the two individuals that abducted and molested your 17 year old daughter two weeks ago; thankfully she is home and safe now. During the criminal's trial, it was brought out that they were frequent subscribers to adult pornographic websites. Ironically, more and more of these so-called pornographic abductions have begun to take place across the country. To help combat this type of crime, and raise the awareness of parents all over the country, you hack into some of the most major and offensive pornographic websites and then leak the names of users over the Internet. Do you believe that this is an unethical privacy violation? Please select one response from below.</p>	.931

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
30	4.83	1.464	2.144	You work in the IS/IT department of a large marketing firm and have access to a huge consumer database that contains information like addresses and emails. You are in your last year of college and money is running tight. Since it will not hurt anyone, you access to corporate database of customers so you can send out emails requesting society's help to get you through college. Do you believe that this is an unethical privacy violation? Please select one response from below.	.929

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
31	5.62	1.023	1.047	You are a network and applications engineer for an organization. While working on the laptop of the director of finance you notice that the laptop contained hundreds of underage pornographic pictures. Knowing that child pornography is illegal, you scan the directors emails to determine if any attachments can be found indicating where these pictures came from, and to determine if the director of finance is doing anything else illegal before reporting this activity to your boss and the authorities. Do you believe that this is an unethical privacy violation? Please select one response from below. Do you believe that this is an unethical privacy violation? Please select one response from below.	.932

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
32	3.43	2.043	4.173	Your parents, spouse, and two children were killed in a car crash by someone authorized to use marijuana by the Medical Marijuana Access Program that is sponsored the government. This is not the first of these types of accidents in the country, but this time the government's program has taken your family members from you. In retaliation, you leak over the Internet the entire database of patient's names who receive medical marijuana. Do you believe that this is an unethical privacy violation?  Please select one response from below.	.931

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
33	5.70	.638	.407	You work for a mobile phone company and saw an advertisement in a newspaper about a car for sale. The car sounded like a good buy. The advertisement listed the seller's mobile phone number, but not the seller's address. Being a system software engineer for the mobile phone company you knew that you could determine the seller's address by accessing the seller's mobile phone records, which you did and went to the seller's house to discuss buying the car. The seller was delighted and the sale went through. Do you believe that this is an unethical privacy violation? Please select one response from below.	.931

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
34	5.70	.799	.638	Being the good IS/IT practitioner that you are, during your lunch break you search your company's network for security holes. You come across a hole that exposes some form of personally identifiable information for every employee in the company. To determine the severity of the hole, you set out to find exactly what information is being exposed for each of the company's employees even though your boss did not ask you to do this. Your reasoning is to help protect privacy, and look good to your boss when promotion time comes around. Do you believe that this is an unethical privacy violation? Please select one response from below.	.930

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
35	4.21	1.680	2.821	You are a programmer for a mid-sized company that is downsizing the IT department you work in. One more employee will be let go, and it is between you and someone else. You know how to inject code into the other employees programming that would cause their program to malfunction and expose personally identifiable information of the company's clients. You cannot afford to lose your job because your daughter's health is very fragile and she requires specialized medications that you cannot afford without your company's health insurance plan. So you inject the code. Do you believe that this is an unethical privacy violation? Please select one response from below.	.931



**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
36	4.75	1.343	1.804	You work in your local hospitals IS/IT department on patient files. Your father has been in and out of the hospital's emergency room a number of times over the past few months, but when you question him, he says it is no big deal. Your mother passed away last year and both you and your older sister are concerned for your father's health so you log into his patient file to determine his health status. Do you believe that this is an unethical privacy violation? Please select one response from below.	.930

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
37	5.85	.533	.284	You are the only female network engineer among three other male network engineers for a mid-sized company. While working late one night, you notice that your boss has left his computer on. You enter his office to turn off the monitor and find that his email is still open. You notice that one of the email headers is about you so you open the email only to find out that your boss and other male network engineers have been discussing you behind your back in sexually explicit manner. You print out the emails and bring them to the head of human resources the very next day. Do you believe that this is an unethical privacy violation? Please select one response from below.	.932

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
38	5.06	1.365	1.862	You are a IS/IT data analyst at a major casino working after normal business hours to finish an important project that is due the next day. You realize that you are missing data that was originally sent to you by a fellow IS/IT coworker. You inadvertently observed your coworker typing their password several days ago, so you decide to login into the system as them and resend the data to yourself so that you can complete the project. Do you believe that this is an unethical privacy violation? Please select one response from below.	.929

**Appendix O – Privacy Violation Questions Measures of Central Tendency and Cronbach if Question is Deleted (cont.)**

Question Number	$\bar{X}$	$\sigma_2$	$\sigma^2$	Privacy Scenario	Cronbach if item is deleted
39	5.89	.506	.256	<p>You are the chief database architect for the world's largest commercial database on consumers. In essence, you have absolute control over all data. The database contains information on over 500 million active consumers worldwide, and it processes over 2,000 data points' per person each year. Covertly covering your tracks, you leak the entire database to a number of huge companies. For these actions, you are paid nearly 700 million dollars. For legal protection, you immediately leave this country for a country with no extradition treaty with the U.S. Do you believe that this is an unethical privacy violation? Please select one response from below.</p>	.931
40	5.36	1.331	1.773	<p>You log into a university student database to change a coworker's grade from a B+ to an A, because without an A in a particular computer security course your friend will be terminated from his current job. Do you believe that this is an unethical privacy violation? Please select one response from below.</p>	.929

**Appendix P – Privacy Violation Questions Descending Mean Values**

$\bar{X}$	Question Number	$\sigma_2$	$\sigma^2$
1.66	14	2.166	4.69
3.04	1	2.075	4.306
3.19	3	2.458	6.041
3.19	16	1.971	3.887
3.43	32	2.043	4.173
3.87	29	2.219	4.925
4.15	21	1.791	3.208
4.21	35	1.68	2.821
4.51	5	1.694	2.87
4.57	26	1.658	2.75
4.75	36	1.343	1.804
4.83	30	1.464	2.144
4.89	18	1.75	3.064
4.91	19	1.713	2.933
4.94	25	1.703	2.901
4.98	7	1.366	1.865
5.00	2	1.24	1.538
5.06	38	1.365	1.862
5.25	28	1.413	1.996
5.26	22	1.546	2.39
5.36	40	1.331	1.773

**Appendix P – Privacy Violation Questions Descending Mean Values**

$\bar{X}$	Question Number	$\sigma_2$	$\sigma^2$
5.38	17	1.39	1.932
5.4	4	1.062	1.128
5.43	8	1.635	2.673
5.47	11	0.953	0.908
5.51	20	0.973	0.947
5.55	15	1.03	1.06
5.58	12	1.184	1.401
5.62	23	1.096	1.201
5.62	31	1.023	1.047
5.68	13	0.976	0.953
5.7	10	0.54	0.292
5.7	33	0.638	0.407
5.7	34	0.799	0.638
5.74	24	0.655	0.429
5.77	27	0.724	0.525
5.85	6	0.411	0.169
5.85	9	0.456	0.208
5.85	37	0.533	0.284
5.89	39	0.506	0.256

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies**  
**PV = Privacy Violation Number**

PV1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 No Violation	7	13.2	13.2	13.2
	1	6	11.3	11.3	24.5
	2 Minimally Unethical	12	22.6	22.6	47.2
	3	8	15.1	15.1	62.3
	4 Moderately Unethical	5	9.4	9.4	71.7
	5	3	5.7	5.7	77.4
	6 Highly Unethical	12	22.6	22.6	100.0
	Total	53	100.0	100.0	

PV2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2 Minimally Unethical	2	3.8	3.8	3.8
	3	6	11.3	11.3	15.1
	4 Moderately Unethical	10	18.9	18.9	34.0
	5	7	13.2	13.2	47.2
	6 Highly Unethical	28	52.8	52.8	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

**PV3**

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 No Violation	15	28.3	28.3	28.3
	1	2	3.8	3.8	32.1
	2 Minimally Unethical	4	7.5	7.5	39.6
	3	6	11.3	11.3	50.9
	4 Moderately Unethical	5	9.4	9.4	60.4
	5	5	9.4	9.4	69.8
	6 Highly Unethical	16	30.2	30.2	100.0
	Total	53	100.0	100.0	

**PV4**

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2 Minimally Unethical	2	3.8	3.8	3.8
	3	2	3.8	3.8	7.5
	4 Moderately Unethical	5	9.4	9.4	17.0
	5	8	15.1	15.1	32.1
	6 Highly Unethical	36	67.9	67.9	100.0
	Total	53	100.0	100.0	



**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

PV5

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 No Violation	2	3.8	3.8	3.8
	1	1	1.9	1.9	5.7
	2 Minimally Unethical	5	9.4	9.4	15.1
	3	5	9.4	9.4	24.5
	4 Moderately Unethical	9	17.0	17.0	41.5
	5	9	17.0	17.0	58.5
	6 Highly Unethical	22	41.5	41.5	100.0
	Total	53	100.0	100.0	

PV6

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4 Moderately Unethical	1	1.9	1.9	1.9
	5	6	11.3	11.3	13.2
	6 Highly Unethical	46	86.8	86.8	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

		PV7		Valid	Cumulative
		Frequency	Percent	Percent	Percent
Valid	2 Minimally Unethical	5	9.4	9.4	9.4
	3	4	7.5	7.5	17.0
	4 Moderately Unethical	7	13.2	13.2	30.2
	5	8	15.1	15.1	45.3
	6 Highly Unethical	29	54.7	54.7	100.0
	Total	53	100.0	100.0	

		PV8		Valid	Cumulative
		Frequency	Percent	Percent	Percent
Valid	0 No Violation	4	7.5	7.5	7.5
	3	1	1.9	1.9	9.4
	5	3	5.7	5.7	15.1
	6 Highly Unethical	45	84.9	84.9	100.0
	Total	53	100.0	100.0	

		PV9		Valid	Cumulative
		Frequency	Percent	Percent	Percent
Valid	4 Moderately Unethical	2	3.8	3.8	3.8
	5	4	7.5	7.5	11.3
	6 Highly Unethical	47	88.7	88.7	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

		PV10			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4 Moderately Unethical	2	3.8	3.8	3.8
	5	12	22.6	22.6	26.4
	6 Highly Unethical	39	73.6	73.6	100.0
	Total	53	100.0	100.0	

		PV11			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2 Minimally Unethical	1	1.9	1.9	1.9
	3	2	3.8	3.8	5.7
	4 Moderately Unethical	5	9.4	9.4	15.1
	5	8	15.1	15.1	30.2
	6 Highly Unethical	37	69.8	69.8	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

		PV12			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 No Violation	1	1.9	1.9	1.9
	2 Minimally Unethical	1	1.9	1.9	3.8
	3	3	5.7	5.7	9.4
	5	3	5.7	5.7	15.1
	6 Highly Unethical	45	84.9	84.9	100.0
	Total	53	100.0	100.0	

		PV13			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2 Minimally Unethical	2	3.8	3.8	3.8
	3	2	3.8	3.8	7.5
	4 Moderately Unethical	1	1.9	1.9	9.4
	5	1	1.9	1.9	11.3
	6 Highly Unethical	47	88.7	88.7	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

		PV14		Valid	Cumulative
		Frequency	Percent	Percent	Percent
Valid	0 No Violation	26	49.1	49.1	49.1
	1	7	13.2	13.2	62.3
	2 Minimally Unethical	6	11.3	11.3	73.6
	3	2	3.8	3.8	77.4
	4 Moderately Unethical	4	7.5	7.5	84.9
	5	1	1.9	1.9	86.8
	6 Highly Unethical	7	13.2	13.2	100.0
	Total	53	100.0	100.0	

		PV15		Valid	Cumulative
		Frequency	Percent	Percent	Percent
Valid	1	1	1.9	1.9	1.9
	3	3	5.7	5.7	7.5
	4 Moderately Unethical	2	3.8	3.8	11.3
	5	6	11.3	11.3	22.6
	6 Highly Unethical	41	77.4	77.4	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

		PV16		Valid	Cumulative
		Frequency	Percent	Percent	Percent
Valid	0 No Violation	5	9.4	9.4	9.4
	1	7	13.2	13.2	22.6
	2 Minimally Unethical	10	18.9	18.9	41.5
	3	8	15.1	15.1	56.6
	4 Moderately Unethical	7	13.2	13.2	69.8
	5	6	11.3	11.3	81.1
	6 Highly Unethical	10	18.9	18.9	100.0
	Total	53	100.0	100.0	

		PV17		Valid	Cumulative
		Frequency	Percent	Percent	Percent
Valid	0 No Violation	1	1.9	1.9	1.9
	2 Minimally Unethical	3	5.7	5.7	7.5
	3	3	5.7	5.7	13.2
	4 Moderately Unethical	2	3.8	3.8	17.0
	5	2	3.8	3.8	20.8
	6 Highly Unethical	42	79.2	79.2	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

		PV18		Valid	Cumulative
		Frequency	Percent	Percent	Percent
Valid	0 No Violation	1	1.9	1.9	1.9
	1	2	3.8	3.8	5.7
	2 Minimally Unethical	7	13.2	13.2	18.9
	4 Moderately Unethical	6	11.3	11.3	30.2
	5	3	5.7	5.7	35.8
	6 Highly Unethical	34	64.2	64.2	100.0
	Total	53	100.0	100.0	

		PV19		Valid	Cumulative
		Frequency	Percent	Percent	Percent
Valid	0 No Violation	2	3.8	3.8	3.8
	1	1	1.9	1.9	5.7
	2 Minimally Unethical	3	5.7	5.7	11.3
	3	6	11.3	11.3	22.6
	4 Moderately Unethical	3	5.7	5.7	28.3
	5	5	9.4	9.4	37.7
	6 Highly Unethical	33	62.3	62.3	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

		PV20			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2 Minimally Unethical	2	3.8	3.8	3.8
	3	1	1.9	1.9	5.7
	4 Moderately Unethical	3	5.7	5.7	11.3
	5	9	17.0	17.0	28.3
	6 Highly Unethical	38	71.7	71.7	100.0
	Total	53	100.0	100.0	

		PV21			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	5	9.4	9.4	9.4
	2 Minimally Unethical	10	18.9	18.9	28.3
	3	1	1.9	1.9	30.2
	4 Moderately Unethical	12	22.6	22.6	52.8
	5	6	11.3	11.3	64.2
	6 Highly Unethical	19	35.8	35.8	100.0
	Total	53	100.0	100.0	



**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

PV22

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 No Violation	3	5.7	5.7	5.7
	2 Minimally Unethical	1	1.9	1.9	7.5
	3	1	1.9	1.9	9.4
	4 Moderately Unethical	3	5.7	5.7	15.1
	5	8	15.1	15.1	30.2
	6 Highly Unethical	37	69.8	69.8	100.0
	Total	53	100.0	100.0	

PV23

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 No Violation	1	1.9	1.9	1.9
	2 Minimally Unethical	1	1.9	1.9	3.8
	4 Moderately Unethical	4	7.5	7.5	11.3
	5	2	3.8	3.8	15.1
	6 Highly Unethical	45	84.9	84.9	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

PV24

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	1.9	1.9	1.9
	4 Moderately Unethical	3	5.7	5.7	7.5
	5	5	9.4	9.4	17.0
	6 Highly Unethical	44	83.0	83.0	100.0
	Total	53	100.0	100.0	

PV25

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	3	5.7	5.7	5.7
	2 Minimally Unethical	7	13.2	13.2	18.9
	3	1	1.9	1.9	20.8
	4 Moderately Unethical	2	3.8	3.8	24.5
	5	6	11.3	11.3	35.8
	6 Highly Unethical	34	64.2	64.2	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

PV26

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	7.5	7.5	7.5
	2 Minimally Unethical	4	7.5	7.5	15.1
	3	5	9.4	9.4	24.5
	4 Moderately Unethical	9	17.0	17.0	41.5
	5	7	13.2	13.2	54.7
	6 Highly Unethical	24	45.3	45.3	100.0
	Total	53	100.0	100.0	

PV27

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2 Minimally Unethical	1	1.9	1.9	1.9
	4 Moderately Unethical	3	5.7	5.7	7.5
	5	2	3.8	3.8	11.3
	6 Highly Unethical	47	88.7	88.7	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

		PV28			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 No Violation	1	1.9	1.9	1.9
	1	1	1.9	1.9	3.8
	2 Minimally Unethical	2	3.8	3.8	7.5
	3	2	3.8	3.8	11.3
	4 Moderately Unethical	4	7.5	7.5	18.9
	5	7	13.2	13.2	32.1
	6 Highly Unethical	36	67.9	67.9	100.0
	Total	53	100.0	100.0	

		PV29			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 No Violation	6	11.3	11.3	11.3
	1	4	7.5	7.5	18.9
	2 Minimally Unethical	7	13.2	13.2	32.1
	3	5	9.4	9.4	41.5
	4 Moderately Unethical	5	9.4	9.4	50.9
	5	4	7.5	7.5	58.5
	6 Highly Unethical	22	41.5	41.5	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

PV30

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	1.9	1.9	1.9
	2 Minimally Unethical	5	9.4	9.4	11.3
	3	4	7.5	7.5	18.9
	4 Moderately Unethical	9	17.0	17.0	35.8
	5	7	13.2	13.2	49.1
	6 Highly Unethical	27	50.9	50.9	100.0
	Total	53	100.0	100.0	

PV31

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 No Violation	1	1.9	1.9	1.9
	3	1	1.9	1.9	3.8
	4 Moderately Unethical	3	5.7	5.7	9.4
	5	5	9.4	9.4	18.9
	6 Highly Unethical	43	81.1	81.1	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

PV32

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 No Violation	4	7.5	7.5	7.5
	1	8	15.1	15.1	22.6
	2 Minimally Unethical	6	11.3	11.3	34.0
	3	12	22.6	22.6	56.6
	4 Moderately Unethical	3	5.7	5.7	62.3
	5	6	11.3	11.3	73.6
	6 Highly Unethical	14	26.4	26.4	100.0
	Total	53	100.0	100.0	

PV33

---

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	1.9	1.9	1.9
	4 Moderately Unethical	2	3.8	3.8	5.7
	5	9	17.0	17.0	22.6
	6 Highly Unethical	41	77.4	77.4	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

PV34

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2 Minimally Unethical	1	1.9	1.9	1.9
	3	1	1.9	1.9	3.8
	4 Moderately Unethical	2	3.8	3.8	7.5
	5	5	9.4	9.4	17.0
	6 Highly Unethical	44	83.0	83.0	100.0
	Total	53	100.0	100.0	

PV35

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 No Violation	2	3.8	3.8	3.8
	1	1	1.9	1.9	5.7
	2 Minimally Unethical	5	9.4	9.4	15.1
	3	9	17.0	17.0	32.1
	4 Moderately Unethical	14	26.4	26.4	58.5
	5	3	5.7	5.7	64.2
	6 Highly Unethical	19	35.8	35.8	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

PV36

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2 Minimally Unethical	3	5.7	5.7	5.7
	3	8	15.1	15.1	20.8
	4 Moderately Unethical	13	24.5	24.5	45.3
	5	4	7.5	7.5	52.8
	6 Highly Unethical	25	47.2	47.2	100.0
	Total	53	100.0	100.0	

PV37

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	1.9	1.9	1.9
	4 Moderately Unethical	1	1.9	1.9	3.8
	5	3	5.7	5.7	9.4
	6 Highly Unethical	48	90.6	90.6	100.0
	Total	53	100.0	100.0	



**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

PV38

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2 Minimally Unethical	4	7.5	7.5	7.5
	3	6	11.3	11.3	18.9
	4 Moderately Unethical	5	9.4	9.4	28.3
	5	6	11.3	11.3	39.6
	6 Highly Unethical	32	60.4	60.4	100.0
	Total	53	100.0	100.0	

PV39

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	1.9	1.9	1.9
	4 Moderately Unethical	1	1.9	1.9	3.8
	5	1	1.9	1.9	5.7
	6 Highly Unethical	50	94.3	94.3	100.0
	Total	53	100.0	100.0	

**Appendix Q – SMEs Privacy Violation Questions Response Frequencies (cont.)**  
**PV = Privacy Violation Number**

		PV40			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 No Violation	1	1.9	1.9	1.9
	2 Minimally Unethical	2	3.8	3.8	5.7
	3	3	5.7	5.7	11.3
	4 Moderately Unethical	4	7.5	7.5	18.9
	5	3	5.7	5.7	24.5
	6 Highly Unethical	40	75.5	75.5	100.0
	Total	53	100.0	100.0	

## Appendix R – PPVS Hallmark Features Section

### Career – Organizational Values

1. How would you describe the area of technology that you currently work in (*you may select more than one option*)

- |  |  |   |
|--|--|---|
| <input type="checkbox"/> Administrator         | <input type="checkbox"/> Data Modeler          | <input type="checkbox"/> Middleware                             |
| <input type="checkbox"/> Analyst               | <input type="checkbox"/> Data Warehousing      | <input type="checkbox"/> Mobile Apps                            |
| <input type="checkbox"/> Application Developer | <input type="checkbox"/> e-Commerce            | <input type="checkbox"/> Networking                             |
| <input type="checkbox"/> Application Engineer  | <input type="checkbox"/> e-Learning            | <input type="checkbox"/> Operating Systems                      |
| <input type="checkbox"/> Architecture          | <input type="checkbox"/> Email                 | <input type="checkbox"/> Operations                             |
| <input type="checkbox"/> Auditing              | <input type="checkbox"/> Embedded Systems      | <input type="checkbox"/> PC Tech/Support                        |
| <input type="checkbox"/> Auditor               | <input type="checkbox"/> Encryption            | <input type="checkbox"/> Pen Testing                            |
| <input type="checkbox"/> Big Data              | <input type="checkbox"/> Engineer              | <input type="checkbox"/> Privacy                                |
| <input type="checkbox"/> CIO                   | <input type="checkbox"/> Forensics             | <input type="checkbox"/> Professor IS/IT/CS                     |
| <input type="checkbox"/> CISO                  | <input type="checkbox"/> Gaming                | <input type="checkbox"/> Programmer                             |
| <input type="checkbox"/> Cloud                 | <input type="checkbox"/> Geospatial            | <input type="checkbox"/> Project Manager                        |
| <input type="checkbox"/> COBIT                 | <input type="checkbox"/> Governance            | <input type="checkbox"/> Security                               |
| <input type="checkbox"/> Compliance            | <input type="checkbox"/> Healthcare Info. Tech | <input type="checkbox"/> Servers                                |
| <input type="checkbox"/> Computer Repair       | <input type="checkbox"/> Helpdesk              | <input type="checkbox"/> Social Media                           |
| <input type="checkbox"/> Cryptography          | <input type="checkbox"/> Indep. Contractor     | <input type="checkbox"/> Software Developer                     |
| <input type="checkbox"/> Cyber Defense         | <input type="checkbox"/> Info. Assurance       | <input type="checkbox"/> Specialist                             |
| <input type="checkbox"/> Databases             | <input type="checkbox"/> Infrastructure        | <input type="checkbox"/> Systems Designer<br>Planner/Integrator |
| <input type="checkbox"/> Data Center           | <input type="checkbox"/> IT Director           | <input type="checkbox"/> Tech Support                           |
| <input type="checkbox"/> Data Mining           | <input type="checkbox"/> Mgr./Supervisor       | <input type="checkbox"/> Technical Writer                       |

**Appendix R – PPVS Hallmark Features Section (cont.)**

- Virtualization                       Voice (VoIP)                       Web/Internet  
 OTHER (type response below)

2. What industry certifications, if any do you hold? Please fill in the boxes below.

If you do not have any industry certifications please skip this question.

- |                         |                         |                         |
|-------------------------|-------------------------|-------------------------|
| A. <input type="text"/> | F. <input type="text"/> | K. <input type="text"/> |
| B. <input type="text"/> | G. <input type="text"/> | L. <input type="text"/> |
| C. <input type="text"/> | H. <input type="text"/> | M. <input type="text"/> |
| D. <input type="text"/> | I. <input type="text"/> | N. <input type="text"/> |
| E. <input type="text"/> | J. <input type="text"/> | O. <input type="text"/> |

3. How would you describe yourself: as a practitioner, or a professional

- As a practitioner  
 As a professional

4. How many years have you worked in the IS/IT CS field

- 1 – 4 years  
 5 – 9 years  
 10 – 14 years  
 15 – 19 years  
 20+ years

**Appendix R – PPVS Hallmark Features Section (cont.)**

5. Do you belong to a professional organization that is related to your career field, such as the ACM, IEEE, or some other association (Please fill in boxes).

Organization/Association

Organization/Association

Organization/Association

Organization/Association

Organization/Association

Organization/Association

6. I have or have had a role model at work that I would consider to be very ethical

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

7. My integrity at work is paramount to who I am as a person, and how my peers see me

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

**Appendix R – PPVS Hallmark Features Section (cont.)**

8. I consider myself a steward of social responsibility in your career

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

9. My employer is committed to social responsibility for the betterment of society

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

10. I would you report a fellow employee that is acting unethically

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

**Appendix R – PPVS Hallmark Features Section (cont.)**

11. I am satisfied with my current job

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

12. Approximately how many employees work at your organization

- 1000+ employees
- 999 – 750 employees
- 749 – 500 employees
- 499 – 250 employees
- 249 – 100 employees
- 99 – 50 employees
- 1 – 49 employees

13. Are you employed?

- Full Time
- Part Time
- Currently Unemployed

**Appendix R– PPVS Hallmark Features Section (cont.)****Religion and Spirituality**

1. I consider myself to be a religious person

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

2. Overall my religious beliefs are important in my life

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

3. My self-identity is closely oriented towards my religious-identity

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree



**Appendix R – PPVS Hallmark Features Section (cont.)**

4. I often attend religious services

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

5. I consider myself a spiritual person

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

6. Overall my spiritual beliefs are important in my life

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

**Appendix R – PPVS Hallmark Features Section (cont.)**

7. My self-identity is closely oriented towards my spiritual-identity
- Strongly disagree
  - Disagree
  - Somewhat disagree
  - Somewhat agree
  - Agree
  - Strongly agree
8. I often read religious or spiritual materials
- Strongly disagree
  - Disagree
  - Somewhat disagree
  - Somewhat agree
  - Agree
  - Strongly agree
9. I often make sense of things through a religious or spiritual understanding
- Strongly disagree
  - Disagree
  - Somewhat disagree
  - Somewhat agree
  - Agree
  - Strongly agree

**Appendix R – PPVS Hallmark Features Section (cont.)**

10. I often find that I make decisions through my religious or spiritual understandings

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

11. I often feel it is necessary to act duty bound

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

**Appendix R – PPVS Hallmark Features Section (cont.)****Ethics – Training – Awareness**

1. Have you ever had formal ethics training

No

Yes

2. Have you ever taken a computer ethics course or had computer ethics training at work

No

Yes

3. Did you ever take an ethics course in school

No

Yes

4. Does your organization provide ethics awareness training

No

Yes

5. Does your organization have a code of ethics specific to IT employees

No

Yes

6. Have you ever been to an ethics awareness training session or program

No

Yes

7. Does your organization have a formal code of ethics

No

Yes

**Appendix R – PPVS Hallmark Features Section (cont.)**

8. I have carefully read the 10 commandments of computer ethics
- Strongly disagree
  - Disagree
  - Somewhat disagree
  - Somewhat agree
  - Agree
  - Strongly agree
9. If you belong to a professional organization or association that relates to your job, do you remember what the content of the organization or association codes of ethics say? (If you do not belong to a professional organization or association, you may skip this question).
- Strongly disagree
  - Disagree
  - Somewhat disagree
  - Somewhat agree
  - Agree
  - Strongly agree

**Appendix R – PPVS Hallmark Features Section (cont.)**

10. I would report a fellow IS/IT employee to my boss if I knew s/he were making copies of company software and taking it home for personal use

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

11. If I knew that I was going to be laid-off or fired I would take proprietary company information to gain a competitive advantage at my next job

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

**Appendix R – PPVS Hallmark Features Section (cont.)**

12. If you knew that you were going to be fired or laid-off, if anything what would you take with you:

- Database information
- Corporate privileged passwords that you know
- Email server account information
- Company financial data
- Research and development plans
- Proprietary Software
- Human resource records
- Nothing
- Other
- Other
- Other

13. I have used my corporate password to access confidential or sensitive information that I should not be accessing

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

**Appendix R – PPVS Hallmark Features Section (cont.)**

14. I have read other individuals emails at work even though I shouldn't

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree



**Appendix R – PPVS Hallmark Features Section (cont.)****Prosocial Behaviors**

1. I donate my time by volunteering to help a charitable organization(s)

- Always
- Very Often
- Sometimes
- Very Seldom
- Never

2. I donate money to help a charitable organization(s)

- Always
- Very Often
- Sometimes
- Very Seldom
- Never

3. I donate blood

- Always
- Very Often
- Sometimes
- Very Seldom
- Never

**Appendix R – PPVS Hallmark Features Section (cont.)**

4. I donate food to a charity(ies)

- Always
- Very Often
- Sometimes
- Very Seldom
- Never

5. I donate clothes to a charity(ies)

- Always
- Very Often
- Sometimes
- Very Seldom
- Never

6. I give money to a stranger(s)

- Always
- Very Often
- Sometimes
- Very Seldom
- Never

**Appendix R – PPVS Hallmark Features Section (cont.)**

7. I have bought girl scout cookies with the intention of knowing that it supports a good cause

- Always
- Very Often
- Sometimes
- Very Seldom
- Never

8. I feel a strong social responsibility to the community the I live in

- Always
- Very Often
- Sometimes
- Very Seldom
- Never

**Appendix R – PPVS Hallmark Features Section (cont.)****General Demographics**

1. What is your age

- 65+
- 64 – 60 years old
- 59 – 50 years old
- 49 – 40 years old
- 39 – 30 years old
- 29 – 20 years old
- 18 or 19 years old

2. Gender

- Male
- Female

3. Marital Status

- Married
- Single

4. Number of children

- 4+
- 3
- 2
- 1
- 0

**Appendix R – PPVS Hallmark Features Section (cont.)**

5. My religion is:

Agnostic

Jewish

Atheist

Mormon

Baptist

Muslim

Buddhist

Protestant

Catholic

OTHER

Christian

6. Highest level of academic education attained.

High school

College degree

Master's degree

Ph.D.

J.D.

7. What is your household income level

> \$50,000

\$51,000 – \$70,000

\$71,000 – \$90,000

\$91,000 – \$110,000

\$111,000 – \$130,000

\$131,000 – \$150,000

< \$151,000

### Appendix S – PPVS-1 15 Privacy Violations to PII

1. A fellow employee that you have been interested in for some time asks you out. You tell them that you are interested in them also but are busy this weekend. You tell them this so that you can do a background check on them to make sure that there is nothing questionable in their past. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

2. You work in your company's IS/IT department. While walking down a hall one day, you notice one of the company cell phones that all of the executives carry, and it is on the floor. Rather than giving it to the security officer of the IS/IT department you logon to it and bring up the person information so that you can give the cell phone back to the correct person. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix S – PPVS-1 15 Privacy Violations to PII (cont.)**

3. You are the director of all IS/IT services at the same university that your spouse is the chair of the English department. Your spouse calls you and tells you that she has misplaced some personal information for a few professors whose information must go on a federal grant that the English department is applying for, and that the grant must be submitted by the end of the day. You know that she has had all of the professor's identification numbers, Social Security Numbers, and other germane information that she needs to finish the grant. Knowing that she previously had all of this personal information for the professors you log into the appropriate server to get here the information again, even though the university has a protocol for requesting this type of information that is supposed to go through the university's grant writing office.

What would you do? Please select one response from below.






I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix S – PPVS-1 15 Privacy Violations to PII (cont.)**

4. You are the only female network engineer among three other male network engineers for a mid-sized company. While working late one night, you notice that your boss has left his computer on. You enter his office to turn off the monitor and find that his email is still open. You notice that one of the email headers is about you so you open the email only to find out that your boss and other male network engineers have been discussing you behind your back in sexually explicit manner. You print out the emails and bring them to the head of human resources the very next day. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

5. You are an IT supervisor at the university that your child attends. You suspect that the money that you are giving your child to pay for classes is being spent on things other than classes, so you log into your child's student account to determine if in fact they have been registering for classes. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this



**Appendix S – PPVS-1 15 Privacy Violations to PII (cont.)**

6. You log into a university student database to change a coworker's grade from a B+ to an A, because without an A in a particular computer security course your friend will be terminated from his current job. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

7. You are a database engineer who works for one of the three major credit card verification bureaus. A friend moved out of town without giving you a forward address or telephone number, and this person owes you \$10,000. You decide to use your company's database to locate this person and try to get your money back. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix S – PPVS-1 15 Privacy Violations to PII (cont.)**

8. You work in your local hospitals IS/IT department and have access to all the computer systems throughout the hospital. You found out from one of your neighbors that another neighbor is sick and in the hospital, so you log into the patient records system to find out what your neighbor’s ailment is and what room they are in so you can go and visit them. What would you do? Please select one response from below.

I would always do this                      I would probably do this depending on the circumstance                      I am not sure what I would do                      I would probably not do this depending on the circumstance                      I would never do this

9. Your boss, the head of the IT department is no nonsense dictator who really pushes everyone to work hard. For his birthday you get him a really nice pen that you know he will always use that has a small RFID tracking device in it so you know where he always is; this way you and the IT team can take it easy when he is not around. What would you do? Please select one response from below.

I would always do this                      I would probably do this depending on the circumstance                      I am not sure what I would do                      I would probably not do this depending on the circumstance                      I would never do this

**Appendix S – PPVS-1 15 Privacy Violations to PII (cont.)**

10. You and your spouse work for the same company, you in the IS/IT department and your wife in the accounting department. You suspect that the head of the accounting department and your spouse are having an affair. You log into both of their office emails and your spouse's personal email outside of the office to see if you can determine anything. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

11. You are an IS/IT employee on your lunch-break. Your job gives you access to all the company email. Just playing around, and not intending to do any harm you pass time by reading internal company emails. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix S – PPVS-1 15 Privacy Violations to PII (cont.)**

12. A new technology management position will be opening in 6 months with a salary that is \$12,000 over your current salary. You and your spouse desperately need a new vehicle. You have access to the human resources databases. You open the human resources database to examine your co-workers resumes so that you could gain a competitive advantage and get the job. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

13. The company you work for is downsizing the IT department you work in. One more employee will be fired, and it is between you and someone else. You found out that the other employee has AIDS by looking through their personal emails at the office. Would you inform your supervisor of this if you knew it would save your job and you did not have to let anyone know how you actually obtained the information? What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix S – PPVS-1 15 Privacy Violations to PII (cont.)**

14. Your parents, spouse, and two children were killed in a car crash by someone authorized to use marijuana by the Medical Marijuana Access Program that is sponsored the government. This is not the first of these types of accidents in the country, but this time the government's program has taken your family members from you. In retaliation, you leak over the Internet the entire database of patient's names who receive medical marijuana. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix S – PPVS-1 15 Privacy Violations to PII (cont.)**

15. You are the chief database architect for the world’s largest commercial database on consumers. In essence, you have absolute control over all data. The database contains information on over 500 million active consumers worldwide, and it processes over 2,000 data points’ per person each year. Covertly covering your tracks, you leak the entire database to a number of huge companies. For these actions, you are paid nearly 700 million dollars. For legal protection, you immediately leave this country for a country with no extradition treaty with the U.S.

What would you do? Please select one response from below.

- |                          |  |                               |  |                          |
|--------------------------|--|-------------------------------|--|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/>                               | <input type="checkbox"/>      | <input type="checkbox"/>                                   | <input type="checkbox"/> |
| I would always do this   | I would probably do this depending on the circumstance | I am not sure what I would do | I would probably not do this depending on the circumstance | I would never do this    |

### Appendix T – PPVS-2 15 Privacy Violations to PII

1. A fellow employee that you have been interested in for some time asks you out. You tell them that you are interested in them also but are busy this weekend. You tell them this so that you can do a background check on them to make sure that there is nothing questionable in their past. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

2. A fellow IS/IT colleague who is a close friend is out of the office for a week. You left your biometric personal identity information badge at home and need to get into a secure area of the building that your friend also accesses. Your friend left his badge in his desk, and has told you in the past if you need to use his badge to get it out of his desk drawer and use it. You allow him to do the same with your badge. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix T – PPVS-2 15 Privacy Violations to PII (cont.)**

3. You are the director of IS/IT at a company. You suspect one of your employees of unethical behaviors that have to do with emails, so after hours you read the employee's emails so that you have supporting evidence when you go to human resources with the problem. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

4. You work in your company's IS/IT department. While walking down a hall one day, you notice one of the company cell phones that all of the executives carry, and it is on the floor. Rather than giving it to the security officer of the IS/IT department you logon to it and bring up the person information so that you can give the cell phone back to the correct person. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this



**Appendix T – PPVS-2 15 Privacy Violations to PII (cont.)**

5. Your parents, spouse, and two children were killed in a car crash by someone authorized to use marijuana by the Medical Marijuana Access Program that is sponsored the government. This is not the first of these types of accidents in the country, but this time the government's program has taken your family members from you. In retaliation, you leak over the Internet the entire database of patient's names who receive medical marijuana. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix T – PPVS-2 15 Privacy Violations to PII (cont.)**

6. You are one of this country’s brightest network security people. Many of your skills were self-taught by learning to hack networks. The police arrested the two individuals that abducted and molested your 17 year old daughter two weeks ago; thankfully she is home and safe now. During the criminal’s trial, it was brought out that they were frequent subscribers to adult pornographic websites. Ironically, more and more of these so-called pornographic abductions have begun to take place across the country. To help combat this type of crime, and raise the awareness of parents all over the country, you hack into some of the most major and offensive pornographic websites and then leak the names of users over the Internet. What would you do?

Please select one response from below.

- |                          |  |                               |  |                          |
|--------------------------|--|-------------------------------|--|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/>                               | <input type="checkbox"/>      | <input type="checkbox"/>                                   | <input type="checkbox"/> |
| I would always do this   | I would probably do this depending on the circumstance | I am not sure what I would do | I would probably not do this depending on the circumstance | I would never do this    |

**Appendix T – PPVS-2 15 Privacy Violations to PII (cont.)**

7. You are the director of all IS/IT services at the same university that your spouse is the chair of the English department. Your spouse calls you and tells you that she has misplaced some personal information for a few professors whose information must go on a federal grant that the English department is applying for, and that the grant must be submitted by the end of the day. You know that she has had all of the professor's identification numbers, Social Security Numbers, and other germane information that she needs to finish the grant. Knowing that she previously had all of this personal information for the professors you log into the appropriate server to get here the information again, even though the university has a protocol for requesting this type of information that is supposed to go through the university's grant writing office.

What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix T – PPVS-2 15 Privacy Violations to PII (cont.)**

8. You are a programmer for a mid-sized company that is downsizing the IT department you work in. One more employee will be let go, and it is between you and someone else. You know how to inject code into the other employees programming that would cause their program to malfunction and expose personally identifiable information of the company's clients. You cannot afford to lose your job because your daughter's health is very fragile and she requires specialized medications that you cannot afford without your company's health insurance plan. So you inject the code. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

9. You are an IT supervisor at the university that your child attends. You suspect that the money that you are giving your child to pay for classes is being spent on things other than classes, so you log into your child's student account to determine if in fact they have been registering for classes. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix T – PPVS-2 15 Privacy Violations to PII (cont.)**

10. You work at a nearby hospital as a network engineer, and are taking databases courses at night. One day on your lunch break, you begin practicing your data mining and extraction skills by developing a query that extracts information for patients who were admitted to the hospital over the past year. You tell the query to include patient name, SSN#, gender, date of admission, home address, phone number, health insurance provider... However, since this information will never be used for anything, and you are the only one that will ever see the information, you assume it is fine to practice your new skills this way. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

11. You work in your local hospital's IS/IT department on patient files. Your father has been in and out of the hospital's emergency room a number of times over the past few months, but when you question him, he says it is no big deal. Your mother passed away last year and both you and your older sister are concerned for your father's health so you log into his patient file to determine his health status. Do you believe that this is an unethical privacy violation? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix T – PPVS-2 15 Privacy Violations to PII (cont.)**

12. You work in the IS/IT department of a large marketing firm and have access to a huge consumer database that contains information like addresses and emails. You are in your last year of college and money is running tight. Since it will not hurt anyone, you access to corporate database of customers so you can send out emails requesting society's help to get you through college. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

13. You work in your university's IS/IT department. The university is withholding your sister's diploma due to a late fee on a library book that you know she never checked out. So you access your sister's school records to erase the fine so that she can graduate, especially since the action would not hurt anyone. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix T – PPVS-2 15 Privacy Violations to PII (cont.)**

14. You have been told that when you finish your master's degree in management and information systems you will be given an assistant director's position within the IS/IT department. Your database course has a capstone project due at the end of the semester. The project is to put together a database with consumer's marketing information that identifies individuals by name, email address, their zip code, and other personal information. Since you are not sure how to do this, you ask your friend who is one of the company's database programmers to help you compile the information using data from the company that you work for so you can turn it in as part of your capstone project. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

15. You know that your job might be at risk, so you to take the pre-emptive move of downloading your company's sensitive and private information to help you gain a competitive advantage at securing a new position with a different company. What would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

### Appendix U – PPVS-3 15 Privacy Violations to PII

1. A fellow employee that you have been interested in for some time asks you out. You tell them that you are interested in them also but are busy this weekend. You tell them this so that you can do a background check on them to make sure that there is nothing questionable in their past. If no one could ever find out that you did this, what would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

2. A fellow IS/IT colleague who is a close friend is out of the office for a week. You left your biometric personal identity information badge at home and need to get into a secure area of the building that your friend also accesses. Your friend left his badge in his desk, and has told you in the past if you need to use his badge to get it out of his desk drawer and use it. You allow him to do the same with your badge. If no one could ever find out that you did this, what would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this



**Appendix U – PPVS-3 15 Privacy Violations to PII (cont.)**

3. You are the director of IS/IT at a company. You suspect one of your employees of unethical behaviors that have to do with emails, so after hours you read the employee's emails so that you have supporting evidence when you go to human resources with the problem. If no one could ever find out that you did this, what would you do? Please select one response from below.

I would always do this	I would probably do this depending on the circumstance	I am not sure what I would do	I would probably not do this depending on the circumstance	I would never do this
---------------------------	---	-------------------------------------	--	--------------------------

4. You work in your company's IS/IT department. While walking down a hall one day, you notice one of the company cell phones that all of the executives carry, and it is on the floor. Rather than giving it to the security officer of the IS/IT department you logon to it and bring up the person information so that you can give the cell phone back to the correct person. If no one could ever find out that you did this, what would you do? Please select one response from below.

I would always do this	I would probably do this depending on the circumstance	I am not sure what I would do	I would probably not do this depending on the circumstance	I would never do this
---------------------------	---	-------------------------------------	--	--------------------------

**Appendix U – PPVS-3 15 Privacy Violations to PII (cont.)**

5. Your parents, spouse, and two children were killed in a car crash by someone authorized to use marijuana by the Medical Marijuana Access Program that is sponsored the government. This is not the first of these types of accidents in the country, but this time the government’s program has taken your family members from you. In retaliation, you leak over the Internet the entire database of patient’s names who receive medical marijuana. If no one could ever find out that you did this, what would you do? Please select one response from below.

- |                        |  |                               |  |                       |
|------------------------|--|-------------------------------|--|-----------------------|
| I would always do this | I would probably do this depending on the circumstance | I am not sure what I would do | I would probably not do this depending on the circumstance | I would never do this |
|------------------------|--|-------------------------------|--|-----------------------|

**Appendix U – PPVS-3 15 Privacy Violations to PII (cont.)**

6. You are one of this country's brightest network security people. Many of your skills were self-taught by learning to hack networks. The police arrested the two individuals that abducted and molested your 17 year old daughter two weeks ago; thankfully she is home and safe now. During the criminal's trial, it was brought out that they were frequent subscribers to adult pornographic websites. Ironically, more and more of these so-called pornographic abductions have begun to take place across the country. To help combat this type of crime, and raise the awareness of parents all over the country, you hack into some of the most major and offensive pornographic websites and then leak the names of users over the Internet. If no one could ever find out that you did this, what would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix U – PPVS-3 15 Privacy Violations to PII (cont.)**

7. You are the director of all IS/IT services at the same university that your spouse is the chair of the English department. Your spouse calls you and tells you that she has misplaced some personal information for a few professors whose information must go on a federal grant that the English department is applying for, and that the grant must be submitted by the end of the day. You know that she has had all of the professor's identification numbers, Social Security Numbers, and other germane information that she needs to finish the grant. Knowing that she previously had all of this personal information for the professors you log into the appropriate server to get here the information again, even though the university has a protocol for requesting this type of information that is supposed to go through the university's grant writing office. If no one could ever find out that you did this, what would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix U – PPVS-3 15 Privacy Violations to PII (cont.)**

8. You are a programmer for a mid-sized company that is downsizing the IT department you work in. One more employee will be let go, and it is between you and someone else. You know how to inject code into the other employees programming that would cause their program to malfunction and expose personally identifiable information of the company's clients. You cannot afford to lose your job because your daughter's health is very fragile and she requires specialized medications that you cannot afford without your company's health insurance plan. So you inject the code. If no one could ever find out that you did this, what would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

9. You are an IT supervisor at the university that your child attends. You suspect that the money that you are giving your child to pay for classes is being spent on things other than classes, so you log into your child's student account to determine if in fact they have been registering for classes. If no one could ever find out that you did this, what would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix U – PPVS-3 15 Privacy Violations to PII (cont.)**

10. You work at a nearby hospital as a network engineer, and are taking databases courses at night. One day on your lunch break, you begin practicing your data mining and extraction skills by developing a query that extracts information for patients who were admitted to the hospital over the past year. You tell the query to include patient name, SSN#, gender, date of admission, home address, phone number, health insurance provider... However, since this information will never be used for anything, and you are the only one that will ever see the information, you assume it is fine to practice your new skills this way. If no one could ever find out that you did this, what would you do? Please select one response from below.

- |                          |  |                               |  |                          |
|--------------------------|--|-------------------------------|--|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/>                               | <input type="checkbox"/>      | <input type="checkbox"/>                                   | <input type="checkbox"/> |
| I would always do this   | I would probably do this depending on the circumstance | I am not sure what I would do | I would probably not do this depending on the circumstance | I would never do this    |

**Appendix U – PPVS-3 15 Privacy Violations to PII (cont.)**

11. You work in your local hospitals IS/IT department on patient files. Your father has been in and out of the hospital's emergency room a number of times over the past few months, but when you question him, he says it is no big deal. Your mother passed away last year and both you and your older sister are concerned for your father's health so you log into his patient file to determine his health status. If no one could ever find out that you did this, what would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

12. You work in the IS/IT department of a large marketing firm and have access to a huge consumer database that contains information like addresses and emails. You are in your last year of college and money is running tight. Since it will not hurt anyone, you access to corporate database of customers so you can send out emails requesting society's help to get you through college. If no one could ever find out that you did this, what would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

**Appendix U – PPVS-3 15 Privacy Violations to PII (cont.)**

13. You work in your university's IS/IT department. The university is withholding your sister's diploma due to a late fee on a library book that you know she never checked out. So you access your sister's school records to erase the fine so that she can graduate, especially since the action would not hurt anyone. If no one could ever find out that you did this, what would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this

14. You have been told that when you finish your master's degree in management and information systems you will be given an assistant director's position within the IS/IT department. Your database course has a capstone project due at the end of the semester. The project is to put together a database with consumer's marketing information that identifies individuals by name, email address, their zip code, and other personal information. Since you are not sure how to do this, you ask your friend who is one of the company's database programmers to help you compile the information using data from the company that you work for so you can turn it in as part of your capstone project. If no one could ever find out that you did this, what would you do? Please select one response from below.

I would always  
do this

I would  
probably do this  
depending on  
the circumstance

I am not sure  
what I would  
do

I would  
probably not do  
this depending  
on the  
circumstance

I would never  
do this



**Appendix U – PPVS-3 15 Privacy Violations to PII (cont.)**

15. You know that your job might be at risk, so you to take the pre-emptive move of downloading your company’s sensitive and private information to help you gain a competitive advantage at securing a new position with a different company. If no one could ever find out that you did this, what would you do? Please select one response from below.

- |                          |  |                               |  |                          |
|--------------------------|--|-------------------------------|--|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/>                               | <input type="checkbox"/>      | <input type="checkbox"/>                                   | <input type="checkbox"/> |
| I would always do this   | I would probably do this depending on the circumstance | I am not sure what I would do | I would probably not do this depending on the circumstance | I would never do this    |

### **Appendix V – Survey Participation Email Invitation Letter**

Thank you so much for accepting my LinkedIn connection invitation. Hello, my name is Mark Rosenbaum and I am finishing my dissertation research for my Ph.D. in information systems science and information privacy at Nova Southeastern University in Fort Lauderdale, Florida. Part of my research, entails collecting survey data from technology professional's regarding their views about information privacy. If it would not be too much of an imposition, I was wondering if you would consider completing the survey to help me with my dissertation research. Most people have found that it takes about 10 to 12 minutes to complete the survey. The survey contains a number of general demographic questions and 15 privacy questions. While your name and email address (e.g., LinkedIn or personal email address) was used to contact you, none of your response data will specifically link you to the results of your survey participation. That is to say, your responses are “completely anonymous”, and can in no way be linked to you as a person, or the company that you work for. I would greatly appreciate your participation. If you are willing to participate, you can cut and paste the following link below into any browser and it will take you to the survey. If you have colleagues in the technology fields that you think might also be willing to lend a hand, please do forward them the link.

Thank you for your consideration.

SURVEY LINK: [REMOVED]

Mark H. Rosenbaum  
[mrosenba@nova.edu](mailto:mrosenba@nova.edu)

Dissertation Chair  
Dr. Ling Wang  
[lingwang@nova.edu](mailto:lingwang@nova.edu)

**Appendix W – Survey Invite Email Distributed by CIOs, CISOs, and CPOs**

This email is being forwarded to you from [Person's Name] who is assisting a university colleague with data collection for his dissertation and Ph.D.

Hello, my name is Mark Rosenbaum and I am finishing my dissertation research for my Ph.D. in information systems science and information privacy at Nova Southeastern University in Fort Lauderdale, Florida. Part of my research, entails collecting survey data from technology professional's regarding their views about information privacy. If it would not be too much of an imposition, I was wondering if you would consider completing the survey to help me with my dissertation research. Most people have found that it takes about 10 to 12 minutes to complete the survey. The survey contains a number of general demographic questions and 15 privacy questions. *Your responses are "completely anonymous", and can in no way be linked to you as a person, or the company that you work for, this also includes your IP address.* I would greatly appreciate your participation. If you are willing to participate, you can cut and paste the following link below into any browser and it will take you to the survey, or just click on the link below. If you have colleagues in the technology fields that you think might also be willing to lend a hand, please do forward them the link. Thank you for your consideration.

SURVEY LINK: [REMOVED]

Mark H. Rosenbaum  
[mrosenba@nova.edu](mailto:mrosenba@nova.edu)

**Dissertation Chair**  
Dr. Ling Wang  
[lingwang@nova.edu](mailto:lingwang@nova.edu)

### Appendix X – Technology-base Job Titles

Active Directory	Desktop Support	Network Infrastructure
AIX	DHCP	Network Operations
Analyst	Disaster Recovery	Network Security
Apache	Disaster Recovery	Network Specialist
Application Developer	e-Commerce	Network Technician
Backup	e-Learning	Operating Systems
Big Data	E-mail Administrator	Oracle
Bioinformatics	Embedded Systems	PC Support
CEH	Encryption	PC Technician
CGEIT	Firewalls	PCI DSS
CIAS	Flash	Penetration Testing
CIO	Game Developer	PERL
CISA	Governance	Ph.D.
CISO	Healthcare Info. Technologies	Professor
CISSP	Help desk	Programmer
Citrix Architect	HTML	Project Manager
Cloud Computing	IAPP	Python
COBIT	Info. Systems Administrator	Risk
Cold Fusion	Info. Systems Engineer	Routers
Compliance	Information Assurance	SDLC
Computer Forensics	Information System Services	Servers
Computer Repair	Information Systems	SharePoint
CPO	Information Technology	SQL

**Appendix X – Technology-base Job Titles (cont.)**

CRISC	InfoSec	Sun Micro Systems
Cryptography	IS/IT Professional	Technical Trainer
CSS	ISO 27001	Technical Writer
Cyber Analyst	IT Analyst	Technician
Cyber Defense	IT Auditing	Training & Development
Cyber Security	IT Technician	UNIX
Data Analyst	ITIL	Virtualization
Data Center	Linux	VMware
Data Mining	Middleware	VoIP
Data Modeler	Mobile Applications	Web Developer
Data protection	Nanotechnology	Windows
Data Warehousing	Natural Language Processing	Wireless Engineer
Database Analyst	.Net	Wireless Network Admin.
Desktop Coordinator	Network Engineer	

**Appendix Y – LinkedIn International Country Search**

Africa	Greenland	Panama
Argentina	Hungary	Poland
Australia	India	Portugal
Austria	Ireland	Romania
Belgium	Israel	Russia
Brazil	Italy	Scotland
Canada	Jamaica	Singapore
Colombia	Japan	South Africa
Denmark	Korea (South)	Spain
Egypt	Mexico	Sweden
England	Morocco	Switzerland
France	Netherlands	United Kingdom
Germany	New Zealand	United States
Greece	Norway	Vietnam

### Appendix Z – LinkedIn Company Search

3M	Baptist Health Systems	Citrix
Abbott Laboratories	BASF	Cleveland Clinic
Acer	Bayer	Coca-Cola Company
ADP	Bayview Assets	Cognizant Technology
Advanced Micro Devices	Bechtel Corp.	Columbia Broadcasting Corp.
Aetna	Bed Bath & Beyond	Computershare Limited
Aflac	Bell Labs	Compuware
AIA	Bentley Systems	Conoco Phillips
Alcatel-Lucent	Berkshire Hathaway	Costco
Alliance-Boots	Bloomingtons	Cox Communications
Am. Broadcasting Corp.	Blue Cross Blue Shield	Cox Enterprises
Amadeus IT Holdings	Boeing	Criteo
Amazon.com	Bristol-Myers Squibb	Cummins Diesel
American Airlines	British Airways	CVS
American Express	British Petroleum	Daimler Automotive
Apple	Bupa Health Insurance	Dell
Aramark	CA Technologies	Deloitte
Assurant Insurance	Capital One	Delta Airlines
Asus	Cargill	Direct TV
AT&T	Carnival Cruises	Dish Network
Autodesk	CHG Healthcare Services	DoD
AXA	Citigroup	Dow Chemical

**Appendix Z – LinkedIn Company Search (cont.)**

DreamWorks Animation	General Motors	Lloyds Banking Group
Dropbox	Georgia-Pacific, LLC.	Macy's
DuPont	Glaxo Smithkline	Maersk
E.ON	Gordon Food Services	Martin Marietta Materials
EarthLink	HCL Technologies Limited	Mayo Clinic
Edward Jones	Hewlett-Packard	Microsoft
Equifax	Home Depot	Monsanto
Ericsson	Honda	Motorola
Ernst & Young	Honeywell Int'l. Services	NASA
Experian	HSBC	National Broadcasting Company
ExxonMobil	Humana	Nestlé
Facebook	IBM	NetApp
Fannie Mae	ING	Nginx
Federal Express	Intel	NOAA
Fidelity Investments	Intersystems	Nokia
Ford Motor Company	Intuit	Northrop Grumman
Freddie Mac	Iron Mountain	Nova Southeastern University
F-Secure	Jackson Health Systems	Novartis
Garman	JC Penney	Nuance
GDF Suez	Johnson & Johnson	Office Depot
General Electric	Kroger Grocery	OfficeMax
General Mills	Levi Strauss & Company	Oracle



**Appendix Z – LinkedIn Company Search (Cont.)**

Overstock.com	SAS	University of Florida
Pan Pacific	Shell Oil	Ultimate Software
Pepsi Company	Sirius XM Radio	Union Pacific Railroad
Petrobras	Skype	Unisys
Pfizer	SMS Mgt. & Technology	United Airlines
Phillip Morris International	Sony	United Health Group
Pixar Animation	Sun Microsystems	United Technologies
Post Food Services	Symantec	United Parcel Service
Price Waterhouse Coopers	Synopsis	US Airways
Procter & Gamble	Target	Verizon
Publix Grocery	TEKsystems	Visa
Qualcomm	Texas Instruments	Vodafone
Quicken Loans	The Discovery Channel	Volkswagen
Rackspace	The Walt Disney Company	Walgreens
Raytheon	TigerDirect	Walmart
Reyes Holdings	Time Warner	Waste Management Corp.
Royal Caribbean Cruises	T-Mobile	Webroot
Royal Dutch Shell	Toyota	Wells Fargo
RWE	TransUnion	Wix.com
Safeway Grocery	Trend Micro	Xerox
Samsung	Turner Broadcasting	Yandex
Sanofi-Aventis	Twitter	Zappo's and Zurich Ins. Co.

## Appendix AA – SurveyGizmo Participation Introduction

My name is Mark Rosenbaum and I am a doctoral candidate at Nova Southeastern University in Fort Lauderdale, Florida. As part of my dissertation research for my Ph.D., I am collecting survey data. The survey that you have chosen to participate in has to do with information privacy views of technology professionals. Prior to answering 15 very short privacy questions you will be presented with a five section demographics questionnaire that will need to be completed first. The survey takes about 10 to 12 minutes to complete and has 69 questions. While your name and email address (e.g., LinkedIn or personal email address) was used to contact you, none of your data responses will specifically link you to the results of your survey participation. That is to say, your responses are “completely anonymous”, and can in no way be linked to you as a person, or the company that you work for. The survey also has a STOP and START function, so that while taking the survey you can STOP it, and then come back to it – see the link at the top of each survey page. Please keep in mind that while completing the survey, *there are no right or wrong answers, especially for the privacy questions*. At any time while completing the survey you may choose to stop participating by closing out the Web page that the survey is on. However, given that this research will help me earn my Ph.D., my hope is that you will complete the entire survey. Your cooperation is greatly appreciated.

Mark H. Rosenbaum  
[mrosenba@nova.edu](mailto:mrosenba@nova.edu)

**Dissertation Chair**  
Dr. Ling Wang  
[lingwang@nova.edu](mailto:lingwang@nova.edu)

### Appendix AB – PPVS-1 Demographics

<i>Country</i>	Frequency	Percent	Cumulative Percent
United States	160	68.1%	68.1%
Undefined	8	3.4%	71.5%
Germany	5	2.1%	73.6%
Ireland	5	2.1%	75.7%
Russian Federation	5	2.1%	77.9%
United Kingdom	5	2.1%	80.0%
Poland	4	1.7%	81.7%
Israel	3	1.3%	83.0%
Spain	3	1.3%	84.3%
Sweden	3	1.3%	85.5%
Australia	2	0.9%	86.4%
Belgium	2	0.9%	87.2%
Canada	2	0.9%	88.1%
France	2	0.9%	88.9%
Greece	2	0.9%	89.8%
India	2	0.9%	90.6%
Anonymous Proxy	1	0.4%	91.1%
Austria	1	0.4%	91.5%
Belarus	1	0.4%	91.9%
Brazil	1	0.4%	92.3%

**Appendix AB – PPVS-1 Demographics (cont.)**

<i>Country</i>	Frequency	Percent	Cumulative Percent
Croatia	1	0.4%	92.8%
Europe	1	0.4%	93.2%
Hungary	1	0.4%	93.6%
Iceland	1	0.4%	94.0%
Indonesia	1	0.4%	94.5%
Italy	1	0.4%	94.9%
Japan	1	0.4%	95.3%
Luxembourg	1	0.4%	95.7%
Netherlands	1	0.4%	96.2%
Norway	1	0.4%	96.6%
Pakistan	1	0.4%	97.0%
Peru	1	0.4%	97.4%
Portugal	1	0.4%	97.9%
Saudi Arabia	1	0.4%	98.3%
Serbia	1	0.4%	98.7%
Singapore	1	0.4%	99.1%
South Africa	1	0.4%	99.6%
Switzerland	1	0.4%	100.0%
Total	235	100.0%	

**Appendix AB – PPVS-1 Demographics (cont.)**

*Gender*

	Frequency	Percent	Cumulative Percent
Male	212	90.2%	90.2%
Female	23	9.8%	100.0%
Total	235	100.0%	

*Age*

	Frequency	Percent	Cumulative Percent
20-29	14	6.0%	6.0%
30-39	59	25.1%	31.1%
40-49	74	31.5%	62.6%
50-59	68	28.9%	91.5%
60-64	18	7.7%	99.1%
65+	2	.9%	100.0%
Total	235	100.0%	

*Education*

	Frequency	Percent	Cumulative Percent
High school	16	6.8%	6.8%
College degree	89	37.9%	44.7%
Master's degree	95	40.4%	85.1%
Ph. D.	35	14.9%	100.0%
Total	235	100.0%	

**Appendix AB – PPVS-1 Demographics (cont.)**

*Marital Status*

	Frequency	Percent	Cumulative Percent
Married	180	76.6%	76.6
Single	55	23.4%	100.0
Total	235	100.0%	

*Number of Children*

	Frequency	Percent	Cumulative Percent
4+	16	6.8%	6.8%
3	23	9.8%	16.6%
2	67	28.5%	45.1%
1	53	22.6%	67.7%
0	76	32.3%	100.0%
Total	235	100.0%	

*Household Income*

	Frequency	Percent	Cumulative Percent
< \$50,000	13	5.5%	5.5%
\$51,000 - \$70,000	34	14.5%	20.0%
\$71,000 - \$90,000	30	12.8%	32.8%
\$91,000 - \$110,000	36	15.3%	48.1%
\$111,000 - \$130,000	34	14.5%	62.6%
\$131,000 - \$150,000	25	10.6%	73.2%
> \$150,000	63	26.8%	100.0%
Total	235	100.0%	

**Appendix AB – PPVS-1 Demographics (cont.)***Years Employed*

	Frequency	Percent	Cumulative Percent
20+ years	91	38.7%	38.7%
15 - 19 years	62	26.4%	65.1%
10 - 14 years	37	15.7%	80.9%
5 - 9 years	33	14.0%	94.9%
1 - 4 years	12	5.1%	100.0%
Total	235	100.0%	

*Job Description*

	Frequency		Frequency
Administrator	55	Computer Repair	15
Analyst	40	Cryptography	21
Application Developer	43	Cyber Defense	28
Application Engineer	23	Databases	48
Architect	53	Data Center	30
Auditing	20	Data Mining	17
Big Data	22	Data Modeler	14
Auditor	13	Data Warehousing	16
CIO	7	E-commerce	18
CISO	10	E-learning	17
Cloud	37	E-mail	28
COBIT	6	Embedded Systems	9
Compliance	45	Encryption	57

**Appendix AB – PPVS-1 Demographics (cont.)**

<i>Job Description</i>			
	Frequency		Frequency
Engineer	21	Pen Testing	7
Forensics	5	Privacy	28
Gaming	8	Professor IS/IT/CS	21
Geospatial	8	Programmer	40
Governance	23	Project Manager	51
Healthcare Info. Tech.	22	Security	74
Helpdesk	22	Servers	46
Independent Contractor	18	Social Media	10
Information Assurance	32	Software Development	46
Infrastructure	48	Specialist	37
IT Director	22	Sys. Planer Designer Integrator	37
Manager/Supervisor	36	Technical Support Technician	34
Middleware	15	Technology Trainer Development	24
Mobile Applications	18	Technical Writer	27
Networking	58	Virtualization	43
Operating Systems	54	Voice VoIP	14
Operations	50	Webpage Designer/Developer	16
PC Technician/Specialist	18		



### Appendix AB – PPVS-1 Demographics (cont.)

#### *Other Job Descriptions*

	Frequency		Frequency
Assistive Technologies	1	Physical Security	2
Chief Cyber Svs. Strategist	1	Quality Mgt.	1
Info. Security Risk Mgt.	1	Service Mgt. Enterprise	1
IT Financial Mgt.	1	Technical Editor	1
Outsourcing	1	Telecom	1

#### *Industry Certifications*

	Frequency		Frequency
ACA CS3	1	CCIE	1
ACE	1	CCNA	1
ACFE	1	CCNP	9
ASEP	1	CCSK	1
ATSP	1	CCSP	2
BiSL	1	CCVP	1
Borderware Engineer	1	CDCP	1
CAP	2	CDP	1
CBCP	1	CEH	11
CCA	1	CGEIT	1
CCDA	2	Check Point	1
CCDP	1	CHEP	1
CCENT	2	CHFI	1
CCEP	1	CHP	1

**Appendix AB – PPVS-1 Demographics (cont.)**

*Industry Certifications*

	Frequency		Frequency
CHS	2	CPP	2
CIPP	3	CQS	1
CISA	14	CRISC	1
Cisco CCIE R&S	4	CSCS	1
CISM	12	CSM	1
CISS	1	CSP	1
CISSP	38	CTT+	1
CITP	1	CWNA	1
Citrix CCP-N	4	Data Privacy	1
CIWMD	1	Data Warehousing	1
CMMI Certification	1	Dell Certified Tech	1
CNA	1	ECDL Expert	1
CNE	1	Enterasys	2
CNE	1	eTOM	1
CNI	1	FBCS	1
COBIT	2	FCIS 27002	1
CompTIA A+	15	Fortinet Security Professional	1
CompTIA Net +	16	G2700	1
CompTIA Security+	19	GCFA	2
Connectwise	1	GCFE	1
CPHIMS	1	GCIA	1

**Appendix AB – PPVS-1 Demographics (cont.)**

*Industry Certifications*

	Frequency		Frequency
GCIH	2	LPIC1	1
GIAC	1	Madcap Flare	1
GPEN	2	MBCI	1
GREM	1	McAfee	4
GSEC	1	MCAS 2007	1
GSNA	1	MCDBA	1
HP Master Architecture	1	MCDST	2
HPUX	1	MCITP	2
HTML5, JavaScript, CSS3	1	MCM	15
IBM	2	MCNE	1
ISO 27001 Lead Auditor	5	MCP	10
ISO 9001 Lead Auditor	1	MCP+I	3
ISSA	1	MCSA	16
ISSAP	4	MCSE	28
ISSEP	2	MCSM	1
ISSMP	2	MCT	11
ISSP	1	MOS	1
ITIL	30	MPH	1
Java Developer	2	MPM	1
Linux Administration	1	MSDST	1
Linux+	1	MSP	1

**Appendix AB – PPVS-1 Demographics (cont.)**

*Industry Certifications*

	Frequency		Frequency
MTA	1	ScrumMaster	2
MTCNA	1	SCWCD	1
MVP	1	Sigma 6 Black Belt	2
NCDA	1	Sigma 6 Lean Green Belt	1
Netware CNA	1	Sigma 6 Master Black Belt	1
Oracle	6	Sigma 6	1
PCIP	1	Sigma 6 Green Belt	1
PMI	1	Sigma 6 Orange Belt	1
PMP	14	Solaris	1
Prince 2 Foundation	4	SSAE16	1
Puppet Professional	1	SSCP	1
RHCE	4	SSGB	1
RHCSA	3	Sun Solaris 10	1
RHCT	1	TCA	1
SCBCD	1	TOGAF	2
SCJP	2	VMWare	12
SCP	1		

**Appendix AB – PPVS-1 Demographics (cont.)**

*Organization & Association Memberships*

	Frequency		Frequency
AAAI	3	Am. Assoc. of Aeronautics	1
AAAS	1	America's SAP User Group	1
AACC	2	APICS	1
AAPM Global Honorary Advisory Council	2	Arizona Ethics and Compliance Council	1
AAS	1	ASA	2
Abet	2	ASIS	5
ACFE	1	AOGEA	1
ACM	33	ATD	1
AERA	1	Atlanta Java User Group (AJUG)	1
AFCEA	5	Atraxis AG	2
AGORA	2	AUSA	1
AGU	1	AVISA	1
AHIMA	2	British Columbia Library Assoc.	2
AIS	8	British Computer Society	6
AISA	1	Business Continuity Institute	1
AITP	1	Bus. Recovery Planners Assoc.	1
American Society for Quality (ASQ)	1	CATEA	1

**Appendix AB – PPVS-1 Demographics (cont.)**

*Organization & Association Memberships*

	Frequency		Frequency
Cav Systems	1	HP	1
COIT- e_health group	2	IAAP	2
CSA	1	IAHSS	1
CSI	1	IAMCP-WIT	1
CSI	1	IAPP	3
CSI	1	IASA	1
DAMA	1	IdHIMA	2
Data Center Pulse	1	IEEE	36
Digital Forensics Assoc.	1	IETF	2
Digital Processing Sys.	1	IGDA	1
DSI	1	IIA	2
E. I. DuPont	2	IIBA	1
Educause	1	INCOSE	1
EUROMA	1	InfraGard	9
FLGISA	1	InSight	1
Florida Gov't. IS Assoc.	1	Institute of Info. Security Prof.	2
Galileo Hellas	1	IPAA	1
Gartner	1	ISA	2
GL Counsel	1	ISACA	24
HDWA	1	ISC(2)	23
HIMSS	4	ISOC-AC	1

**Appendix AB – PPVS-1 Demographics (cont.)**

*Organization & Association Memberships*

	Frequency		Frequency
ISSA	17	Society of Petroleum Engineers	1
ITFM	1	SPIe	1
ITIL	1	SQL PASS	1
itSMF	2	SunGard - Public Sector	1
Kiros	2	Systems Ltd	1
Mobile Technology Assoc. of Michigan	2	Tampa Microsoft Users Group	1
NH-ISAC	1	Am. Academy of Project. Mgt.	1
OWASP	1	The Green Grid	1
Pakistan Revenue Automation	1	Thinspace	1
RABQSA International	2	TTEC	2
REN-ISAC	1	United Nations Development Programme	1
RESNA	1	Upsilon Pi Epsilon	2
SANS	4	Uptime Institute Network	1
Scrum Alliance	2	USENIX	1
Sec.MN	1	Utilities	1
SIAM	3	VMUG	2
SIM	1	Wireless Broadband Alliance	1
Soc. for Tech. Comm.	3	Women in Technology	1
Soc. of Compliance and Ethics Professionals	1		

### Appendix AC – PPVS-1 Correlations Tables

*PPVS-1 Correlations Table*

		Privacy Score	Religiosity & Spirituality	Prosocial Behavior	Age	Years Worked in IS/IT Field	Consider Myself Ethical Question 7 & 8	Had a Work Role Model or Mentor	Ever Had Ethics Training	Highest level of education	Household income
Pearson Correlation	Privacy Score	1.00	0.23	0.48	0.35	0.38	0.41	0.14	0.21	0.11	0.31
	Religiosity & Spirituality	0.23	1.00	0.47	0.23	0.17	0.29	0.11	0.16	0.09	0.11
	Prosocial Behaviors	0.48	0.47	1.00	0.45	0.37	0.41	0.15	0.30	0.24	0.25
	Age	0.35	0.23	0.45	1.00	0.65	0.29	-0.01	0.12	0.25	0.37
	Yrs. Worked in IS/IT Field	0.38	0.17	0.37	0.65	1.00	0.32	0.14	0.19	0.12	0.51
	Consider Myself Ethical Question 7 & 8	0.41	0.29	0.41	0.29	0.32	1.00	0.31	0.18	0.09	0.24
	Had a Work Role Model or Mentor	0.14	0.11	0.15	-0.01	0.14	0.31	1.00	0.10	0.00	0.07
	Ever Had Ethics Training	0.21	0.16	0.30	0.12	0.19	0.18	0.10	1.00	0.13	0.24
	Highest level of education	0.11	0.09	0.24	0.25	0.12	0.09	0.00	0.13	1.00	0.21
	Household income	0.31	0.11	0.25	0.37	0.51	0.24	0.07	0.24	0.21	1.00



**Appendix AC – PPVS-1 Correlations Tables (cont.)**

*PPVS-1 Correlations Table*

		Privacy Score	Religiosity & Spirituality	Prosocial Behavior	Age	Years Worked in IS/IT Field	Consider Myself Ethical Question 7 & 8	Had a Work Role Model or Mentor	Ever Had Ethics Training	Highest level of education	Household income
Sig. (1-tailed)	Privacy Score	.	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.05	0.00
	Religiosity & Spirituality	0.00	.	0.00	0.00	0.01	0.00	0.05	0.01	0.09	0.05
	Prosocial Behaviors	0.00	0.00	.	0.00	0.00	0.00	0.01	0.00	0.00	0.00
	Age	0.00	0.00	0.00	.	0.00	0.00	0.43	0.04	0.00	0.00
	Yrs. Worked in IS/IT Field	0.00	0.01	0.00	0.00	.	0.00	0.02	0.00	0.04	0.00
	Consider Myself Ethical Question 7 & 8	0.00	0.00	0.00	0.00	0.00	.	0.00	0.00	0.10	0.00
	Had a Work Role Model or Mentor	0.02	0.05	0.01	0.43	0.02	0.00	.	0.07	0.50	0.13
	Ever Had Ethics Training	0.00	0.01	0.00	0.04	0.00	0.00	0.07	.	0.02	0.00
	Highest level of education	0.05	0.09	0.00	0.00	0.04	0.10	0.50	0.02	.	0.00
	Household income	0.00	0.05	0.00	0.00	0.00	0.00	0.13	0.00	0.00	.

**Appendix AC – PPVS-1 Correlations Tables (cont.)**

*PPVS-1 Correlations Table*

		Privacy Score	Religiosity & Spirituality	Prosocial Behavior	Age	Years Worked in IS/IT Field	Consider Myself Ethical Question 7 & 8	Had a Work Role Model or Mentor	Ever Had Ethics Training	Highest level of education	Household income
N	Privacy Score	235	235	235	235	235	233	235	235	235	235
	Religiosity & Spirituality	235	235	235	235	235	233	235	235	235	235
	Prosocial Behaviors	235	235	235	235	235	233	235	235	235	235
	Age	235	235	235	235	235	233	235	235	235	235
	Yrs. Worked in IS/IT Field	235	235	235	235	235	233	235	235	235	235
	Consider Myself Ethical Question 7 & 8	235	235	235	235	235	235	235	235	235	235
	Had a Work Role Model or Mentor	235	235	235	235	235	233	235	235	235	235
	Ever Had Ethics Training	235	235	235	235	235	233	235	235	235	235
	Ever Had Ethics Training	235	235	235	235	235	233	235	235	235	235
	Highest level of education	235	235	235	235	235	233	235	235	235	235
	Household income	235	235	235	235	235	233	235	235	235	235

### Appendix AD – PPVS-2 Demographics

#### *Country*

	Frequency	Percent	Cumulative Percent
United States	172	100.0%	100.0%

#### *Gender*

	Frequency	Percent	Cumulative Percent
Male	109	63.4%	64.4%
Female	63	36.6%	100.0%
Total	172	100.0%	

#### *Age*

	Frequency	Percent	Cumulative Percent
20 - 29 years old	16	9.3%	9.3%
30 - 39 years old	65	37.8%	47.1%
40 - 49 years old	39	22.7%	69.8%
50 - 59 years old	34	19.8%	89.5%
60 - 64 years old	13	7.6%	97.1%
65+	5	2.9%	100.0%
Total	172	100.0%	

#### *Education*

	Frequency	Percent	Cumulative Percent
High school	13	7.6%	7.6%
College degree	98	57.0%	64.6%
Master's degree	57	33.1%	97.7%
Ph.D.	4	2.3%	100.0%
Total	172	100.0%	

**Appendix AD – PPVS-2 Demographics (cont.)**

*Marital Status*

	Frequency	Percent	Cumulative Percent
Married	115	66.9%	66.9%
Single	57	33.1%	100.0%
Total	172	100.0%	

*Number of Children*

	Frequency	Percent	Cumulative Percent
4+	5	2.9%	2.9%
3	16	9.3%	12.2%
2	49	28.5%	40.7%
1	41	23.8%	64.5%
0	61	35.5%	100.0%
Total	172	100.0%	

*Household Income*

	Frequency	Percent	Cumulative Percent
< \$50,000	30	14%	14.0%
\$51,000 - \$70,000	28	5.8%	19.8%
\$71,000 - \$90,000	33	8.1%	27.9%
\$91,000 - \$110,000	33	19.2%	47.1%
\$111,000 - \$130,000	14	19.2%	66.3%
\$131,000 - \$150,000	10	16.3%	82.6%
> \$150,000	24	17.4%	100.0%
Total	172	100.0%	

**Appendix AD – PPVS-2 Demographics (cont.)**

*Years Employed*

	Frequency	Percent	Cumulative Percent
20+ years	20	11.6%	11.6%
15 - 19 years	41	23.8%	35.5%
10 - 14 years	40	23.3%	58.7%
5 - 9 years	24	14.0%	72.7%
1 - 4 years	47	27.3%	100.0%
Total	172	100.0%	

*Job Description*

	Frequency		Frequency
Administrator	23	Computer Repair	16
Analyst	24	Cryptography	3
Application Developer	16	Cyber Defense	3
Application Engineer	10	Databases	20
Architect	4	Data Center	8
Auditing	1	Data Mining	5
Big Data	10	Data Modeler	4
Auditor	2	Data Warehousing	10
CIO	4	E-commerce	10
CISO	0	E-learning	4
Cloud	8	E-mail	17
COBIT	0	Embedded Systems	3
Compliance	2	Encryption	4

**Appendix AD – PPVS-2 Demographics (cont.)**

<i>Job Description</i>			
	Frequency		Frequency
Engineer	18	Pen Testing	4
Forensics	0	Privacy	4
Gaming	3	Professor IS/IT/CS	5
Geospatial	1	Programmer	21
Governance	3	Project Manager	21
Healthcare Info. Tech.	7	Security	16
Helpdesk	18	Servers	18
Independent Contractor	3	Social Media	2
Information Assurance	5	Software Development	29
Infrastructure	8	Specialist	7
IT Director	33	Sys. Planer Designer Integrator	12
Manager/Supervisor	15	Technical Support Technician	22
Middleware	2	Technology Trainer Development	5
Mobile Applications	6	Technical Writer	2
Networking	24	Virtualization	10
Operating Systems	19	Voice VoIP	8
Operations	19	Webpage Designer/Developer	21
PC Technician/Specialist	28		

**Appendix AD – PPVS-2 Demographics (cont.)**

*Industry Certifications*

	Frequency		Frequency
C++	1	HTML	1
CAST	1	IBM	1
CCA	1	IBM MQ Series Admin.	1
CCDP	1	ITIL Foundations	4
CCNA	6	J2EE	1
CCNP	2	Java	2
CDP	2	Juniper	1
Cisco	7	loma	1
CISSP	2	MCE	1
Citrix	1	MCP	1
CIW	1	MCSA	1
CNE	1	MCSE	11
CompTIA A+	15	Microsoft Non-disclosed	6
CompTIA N+	10	Microsoft DBA	1
CompTIA Security+	5	Microsoft SBS	1
Compuware APM	1	Oracle	7
CPP	1	PeopleSoft PeopleTools	1
GSEC	1	PMP	8
GSLC	1	Prince2	1
HP	1	SAP certified	1
HP Loadrunner Specialist	1	Scrum Master	2

**Appendix AD – PPVS-2 Demographics (cont.)**

<i>Organization &amp; Association Members</i>			
	Frequency		Frequency
AAAS	1	IEEE	6
ACUTA	1	Infragard	1
AITP	1	LOPSA	1
Apple	1	NAP	1
ASQ	1	NBFA	1
Association of Certified Fraud Examiners	1	PMI	7
ASUG	1	SDF	1
CDIA	1	SIMGHOSTS	1
Cisco	1	SIMposium	1
Citrix	1	Soc. of Compliance and Ethics Professionals	1
CTS	1	Society for Simulation in Healthcare	1
DRI	1	SWE	1
Foundation Information Systems Managers	1	Technology Affinity Group of the Council on Foundations	1
HP	1	Wipro	1
IBM	2	Women in Technology Int'l	1



**Appendix AE – PPVS-2 Correlations Tables**

*PPVS-2 Correlations Table*

		Privacy Score	Religiosity & Spirituality	Prosocial Behavior	Age	Years Worked in IS/IT Field	Consider Myself Ethical Question 7 & 8	Had a Work Role Model or Mentor	Ever Had Ethics Training	Highest level of education	Household income
Pearson Correlation	Privacy Score	1.00	-0.03	-0.08	0.23	-0.22	0.10	0.03	-0.01	-0.08	-0.04
	Religiosity & Spirituality	-0.03	1.00	0.21	-0.04	-0.01	0.16	0.17	0.20	0.11	-0.04
	Prosocial Behaviors	-0.08	0.21	1.00	-0.06	-0.08	0.34	0.30	0.18	0.22	0.17
	Age	0.23	-0.04	-0.06	1.00	-0.64	-0.02	-0.05	-0.05	0.03	0.12
	Yrs. Worked in IS/IT Field	-0.22	-0.01	-0.08	-0.64	1.00	0.03	-0.02	0.00	-0.12	-0.31
	Consider Myself Ethical Question 7 & 8	0.10	0.16	0.34	-0.02	0.03	1.00	0.46	0.12	0.01	0.00
	Had a Work Role Model or Mentor	0.03	0.17	0.30	-0.05	-0.02	0.46	1.00	0.18	0.06	0.07
	Ever Had Ethics Training	-0.01	0.20	0.18	-0.05	0.00	0.12	0.18	1.00	0.21	0.06
	Highest level of education	-0.08	0.11	0.22	0.03	-0.12	0.01	0.06	0.21	1.00	0.29
	Household income	-0.04	-0.04	0.17	0.12	-0.31	0.00	0.07	0.06	0.29	1.00

**Appendix AE – PPVS-2 Correlations Tables (cont.)**

*PPVS-2 Correlations Table*

	Privacy Score	Religiosity & Spirituality	Prosocial Behavior	Age	Years Worked in IS/IT Field	Consider Myself Ethical Question 7 & 8	Had a Work Role Model or Mentor	Ever Had Ethics Training	Highest level of education	Household income
Sig. (1-tailed)										
Privacy Score		0.33	0.15	0.00	0.00	0.10	0.36	0.45	0.16	0.28
Religiosity & Spirituality	0.33		0.00	0.30	0.43	0.02	0.01	0.00	0.07	0.32
Prosocial Behaviors	0.15	0.00		0.21	0.16	0.00	0.00	0.01	0.00	0.01
Age	0.00	0.30	0.21		0.00	0.40	0.27	0.24	0.33	0.06
Yrs. Worked in IS/IT Field	0.00	0.43	0.16	0.00		0.35	0.41	0.50	0.06	0.00
Consider Myself Ethical Question 7 & 8	0.10	0.02	0.00	0.40	0.35		0.00	0.06	0.44	0.49
Had a Work Role Model or Mentor	0.36	0.01	0.00	0.27	0.41	0.00		0.01	0.23	0.17
Ever Had Ethics Training	0.45	0.00	0.01	0.24	0.50	0.06	0.01		0.00	0.21
Highest level of education	0.16	0.07	0.00	0.33	0.06	0.44	0.23	0.00		0.00
Household income	0.28	0.32	0.01	0.06	0.00	0.49	0.17	0.21	0.00	



### Appendix AF – PPVS-3 Demographics

<i>Country</i>	Frequency	Percent	Cumulative Percent
Argentina	1	.6%	0.6%
Australia	2	1.2%	1.8%
Austria	1	0.6%	2.4%
Belarus	1	0.6%	3.0%
Brazil	1	0.6%	3.6%
Bulgaria	2	1.2%	4.8%
Canada	1	0.6%	5.4%
Egypt	3	1.8%	7.2%
France	3	1.8%	9.0%
Germany	1	0.6%	9.6%
Iceland	1	0.6%	10.2%
India	1	0.6%	10.8%
Israel	3	1.8%	12.7%
Malaysia	1	0.6%	13.3%
Pakistan	1	0.6%	13.9%
Panama	1	0.6%	14.5%
Poland	1	0.6%	15.1%
Portugal	1	0.6%	15.7%
Proxy Server	7	4.2%	19.9%
Russian Federation	2	1.2%	21.1%
Serbia	1	0.6%	21.7%
Singapore	4	2.4%	24.1%

**Appendix AF – PPVS-3 Demographics (cont.)**

<i>Country (cont.)</i>			
	Frequency	Percent	Cumulative Percent
Spain	1	0.6%	24.7%
Sweden	1	0.6%	25.3%
Switzerland	3	1.8%	27.1%
Taiwan	1	0.6%	27.7%
United Kingdom	11	6.6%	34.3%
United States	109	65.7%	100.0%
Total	166	100.0%	

<i>Gender</i>			
	Frequency	Percent	Cumulative Percent
Male	141	84.9%	84.9%
Female	25	15.1%	100.0%
Total	166	100.0%	

<i>Age</i>			
	Frequency	Percent	Cumulative Percent
18-19 years old	1	0.6%	0.6%
20-29 years old	27	16.3%	16.9%
30-39 years old	49	29.5%	46.4%
40-49years old	50	30.1%	76.5%
50-59 years old	36	21.7%	98.2%
60-64 years old	2	1.2%	99.4%
65+ years old	1	0.6%	100.0%
Total	166	100.0%	

**Appendix AF – PPVS-3 Demographics (cont.)***Education*

	Frequency	Percent	Cumulative Percent
High school	27	16.3%	16.3%
College degree	78	47.0%	63.3%
Master's degree	53	31.9%	95.2%
Ph.D.	8	4.8%	100.0%
Total	166	100.0%	

*Marital Status*

	Frequency	Percent	Cumulative Percent
Married	121	72.9%	72.9%
Single	45	27.1%	100.0%
Total	166	100.0%	

*Number of Children*

	Frequency	Percent	Cumulative Percent
4+	10	6.0%	6.0%
3	24	14.5%	20.5%
2	46	27.7%	48.2%
1	34	20.5%	68.7%
0	52	31.3%	100.0%
Total	166	100.0%	

**Appendix AF – PPVS-3 Demographics (cont.)**

<i>Household Income</i>			
	Frequency	Percent	Cumulative Percent
< \$50,000	20	12.0%	12.0%
\$51,000 - \$70,000	25	15.1%	27.1%
\$71,000 - \$90,000	16	9.6	36.7%
\$91,000 - \$110,000	33	19.9	56.6%
\$111,000 - \$130,000	23	13.9	70.5%
\$131,000 - \$150,000	9	5.4	75.9%
> \$150,000	40	24.1	100.0%
Total	166	100.0	

<i>Years Employed</i>			
	Frequency	Percent	Cumulative Percent
20+ years	12	7.2%	7.2%
15 - 19 years	43	25.9%	33.1%
10 - 14 years	32	19.3%	52.4%
5 - 9 years	31	18.7%	71.1%
1 - 4 years	48	28.9%	100.0%
Total	166	100.0%	

**Appendix AF – PPVS-3 Demographics (cont.)**

<i>Job Description</i>			
	Frequency		Frequency
Administrator	41	E-commerce	16
Analyst	34	E-learning	3
Application Developer	21	E-mail	7
Application Engineer	9	Embedded Systems	5
Architect	33	Encryption	18
Auditing	11	Engineer	22
Big Data	13	Forensics	10
Auditor	3	Gaming	2
CIO	3	Geospatial	0
CISO	6	Governance	8
Cloud	10	Healthcare Info. Technologies	9
COBIT	2	Helpdesk	22
Compliance	21	Independent Contractor	8
Computer Repair	4	Information Assurance	16
Cryptography	19	Infrastructure	35
Cyber Defense	24	IT Director	11
Databases	19	Manager Supervisor	16
Data Center	9	Middleware	4
Data Mining	9	Mobile Applications	8
Data Modeler	6	Networking	40
Data Warehousing	7	Operating Systems	44



**Appendix AF – PPVS-3 Demographics (cont.)***Job Description (cont.)*

	Frequency		Frequency
Operations	27	Software Development	27
PC Technician Specialist	23	Specialist	26
Pen Testing	14	Systems Planner Designer Integrator	17
Privacy	12	Technical Support Technician	34
Professor IS/IT/CS	6	Technology Trainer Development	9
Programmer	20	Technical Writer	4
Project Manager	23	Virtualization	11
Security	48	Voice VoIP	9
Servers	26	Webpage Designer/Developer/Admin	7
Social Media	5		

*Other Job Descriptions*

	Frequency		Frequency
Business Continuity	1	Telecommunications	1
Data Migration	1	User-Centered Design	1

**Appendix AF – PPVS-3 Demographics (cont.)**

*Industry Certifications*

	Frequency		Frequency
3COM VoIP	1	CGEIT	3
ACE	1	Check Point - CCSA	1
ACMT	1	Check Point - CCSE	1
ACSP 10.7	1	CIA	1
ACTC 10.6	1	CICA	1
Adobe ColdFusion	1	CICSP	1
Apple Deployment 10.6	1	CIMP	1
Apple Security & Mobility	1	CIPM	1
BCS CITP	1	CIPP/US	2
BlackBerry Ent. Server	1	CIPT	2
BSNL	1	CISA	9
CBAP	1	CCDA	1
CCAA	1	CCNA Data Center	4
CCAI	1	CCNP R&S	1
CCIE	1	CISM	8
CCISO	1	CISSP	11
CCNA	7	Certified Admin Apache	1
CCSE	1	CMDBA (MySQL)	1
CEH	3	CNA	1
Certificate Proj. Manager	1	Cognos analysis studio	1
CFE	1	CompTIA A+	16

### Appendix AF – PPVS-3 Demographics (cont.)

<i>Industry Certifications</i>			
	Frequency		Frequency
CompTIA Linux+	1	GSLC	1
CompTIA N+	12	GWAPT	1
CompTIA Security+	8	GXPN	1
CQA	1	HL7	1
CQAR	1	HP AIS Network Automation V9	1
CRISC	3	IBM Websphere App. Server	1
CSEC	1	IBM Websphere Message Queue	1
CSSA	1	i-Net +	1
DataCore SANMelody	1	ISC2 CSSLP	1
Storage Virtualization	1	ISEB	1
Dell Certifications	1		
EMCDSA	1	ISO 20000	1
EMCPA	1	ISO 27002 Lead Implementer	1
FLMI	1	ITIL	12
GCED	1	Java Programmer	1
GCIH	4	Java Software Developer	1
GCUX	1	JNCIA	1
GIAC	1	Linux Virtualization	1
GISP	1	MCDBA	1
GLEG	1	MCDST	1
GPEN	2	MCITP	4
GSEC	5	MCP	7

**Appendix AF – PPVS-3 Demographics (cont.)**

<i>Industry Certifications</i>			
	Frequency		Frequency
MCSA	3	QA/R	1
MCSA	1	RHCA	1
MCSE	7	RHCDS	1
Microsoft Nondisclosed	3	RHCE	6
MCTS	4	SAS Developer	1
MongoDB DBA	1	Scrum Master	1
MOS SharePoint 2010	1	Six Sigma Black Belt	1
OCP Oracle 7	1	SonicWall Firewalls	1
Oracle	1	SSCP	2
Oracle Java Programmer	1	VCA5-DCV	3
PERL	2	VMWare Infrastructure 3.5	1
PMP	5	Weblogic Developer	1
Polycomm Systems Cert.	1	XenServer Virtualization	1
PRINCE2	1		

**Appendix AF – PPVS-3 Demographics (cont.)**

<i>Organization &amp; Association Memberships</i>			
	Frequency		Frequency
ACAMS	1	HFMA	1
ACM	4	HIMSS	2
AFCEA	1	IAA	1
AGAP2	1	IAPP	2
Agile Alliance	1	ICTFF	1
AICPA	1	IDF	1
AIS	3	IEEE	1
AMIA	1	IIA	4
Android Dev Group MV	1	IIBA	1
ASQ	1	Infragard	5
ATD	1	ISA	1
BIC	1	ISACA	15
British Computer Society	1	ISC2	7
CIOLN	1	ISO/IEC JTC1/SC27	1
CISO Executive Network	1	ISO27001	1
Cloud Computing Consortium	1	ISSA	4
CPIC	1	NABA	1
CT163	1	NACD	1
FENG	1	PCM	1
FSISAC	1	PMI	7
Google Developers Group SV	1	RIPE	1

### Appendix AG – PPVS-3 Correlations Tables

*PPVS-3 Correlations Table*

		Privacy Score	Religiosity & Spirituality	Prosocial Behavior	Age	Years Worked in IS/IT Field	Consider Myself Ethical Question 7 & 8	Had a Work Role Model or Mentor	Ever Had Ethics Training	Highest level of education	Household income
Pearson Correlation	Privacy Score	1.00	0.27	0.49	0.29	-0.19	0.24	0.14	0.28	-0.08	0.23
	Religiosity & Spirituality	0.27	1.00	0.30	0.06	-0.02	0.15	0.06	0.27	0.07	-0.03
	Prosocial Behaviors	0.49	0.30	1.00	0.20	-0.25	0.23	0.10	0.35	0.13	0.26
	Age	0.29	0.06	0.20	1.00	-0.66	0.15	0.07	0.10	0.15	0.45
	Yrs. Worked in IS/IT Field	-0.19	-0.02	-0.25	-0.66	1.00	-0.21	-0.04	-0.02	-0.09	-0.50
	Consider Myself Ethical Question 7 & 8	0.24	0.15	0.23	0.15	-0.21	1.00	0.41	-0.01	-0.05	0.09
	Had a Work Role Model or Mentor	0.14	0.06	0.10	0.07	-0.04	0.41	1.00	0.05	-0.03	0.12
	Ever Had Ethics Training	0.28	0.27	0.35	0.10	-0.02	-0.01	0.05	1.00	0.07	0.08
	Highest level of education	-0.08	0.07	0.13	0.15	-0.09	-0.05	-0.03	0.07	1.00	0.21
	Household income	0.23	-0.03	0.26	0.45	-0.50	0.09	0.12	0.08	0.21	1.00

**Appendix AG – PPVS-3 Correlations Tables (cont.)**

*PPVS-3 Correlations Table*

	Privacy Score	Religiosity & Spirituality	Prosocial Behavior	Age	Years Worked in IS/IT Field	Consider Myself Ethical Question 7 & 8	Had a Work Role Model or Mentor	Ever Had Ethics Training	Highest level of education	Household income
Sig. (1-tailed)		0.00	0.00	0.00	0.01	0.00	0.03	0.00	0.15	0.00
	Privacy Score									
	Religiosity & Spirituality	0.00	0.00	0.23	0.40	0.03	0.21	0.00	0.19	0.37
	Prosocial Behaviors	0.00	0.00	0.01	0.00	0.00	0.10	0.00	0.05	0.00
	Age	0.00	0.23	0.01	0.00	0.03	0.17	0.09	0.03	0.00
	Yrs. Worked in IS/IT Field	0.01	0.40	0.00	0.00	0.00	0.28	0.38	0.14	0.00
	Consider Myself Ethical Question 7 & 8	0.00	0.03	0.00	0.03	0.00	0.00	0.44	0.27	0.11
	Had a Work Role Model or Mentor	0.03	0.21	0.10	0.17	0.28	0.00	0.27	0.37	0.06
	Ever Had Ethics Training	0.00	0.00	0.00	0.09	0.38	0.44	0.27	0.20	0.16
	Highest level of education	0.15	0.19	0.05	0.03	0.14	0.27	0.37	0.20	0.00
	Household income	0.00	0.37	0.00	0.00	0.00	0.11	0.06	0.16	0.00

**Appendix AG – PPVS-3 Correlations Tables (cont.)**

*PPVS-3 Correlations Table*

		Privacy Score	Religiosity & Spirituality	Prosocial Behavior	Age	Years Worked in IS/IT Field	Consider Myself Ethical Question 7 & 8	Had a Work Role Model or Mentor	Ever Had Ethics Training	Highest level of education	Household income
N	Privacy Score	166	166	166	166	166	165	166	166	166	166
	Religiosity & Spirituality	166	166	166	166	166	165	166	166	166	166
	Prosocial Behaviors	166	166	166	166	166	165	166	166	166	166
	Age	166	166	166	166	166	165	166	166	166	166
	Yrs. Worked in IS/IT Field	166	166	166	166	166	165	166	166	166	166
	Consider Myself Ethical Question 7 & 8	166	166	166	166	166	166	166	166	166	166
	Had a Work Role Model or Mentor	166	166	166	166	166	165	166	166	166	166
	Ever Had Ethics Training	166	166	166	166	166	165	166	166	166	166
	Highest level of education	166	166	166	166	166	165	166	166	166	166
	Household income	166	166	166	166	166	165	166	166	166	166



## References

- Center for the study of ethics in the professions. (2011). Retrieved February 5, 2012, from [http://ethics.iit.edu/indexOfCodes.php?cat\\_id=6](http://ethics.iit.edu/indexOfCodes.php?cat_id=6)
- Abi-Raad, M. (1999). Codes of ethics? Which one? *ACM SIGCSE Bulletin* 31(2), 73-77.
- ACM. (1992). ACM codes of ethics and professional conduct. Retrieved January 01, 2013 from <http://www.acm.org/about/code-of-ethics>
- Adelson, J. L., & McCoach, D. B. (2010). Measuring the mathematical attitudes of elementary students: The effects of a 4-point or 5-point Likert-type scale. *Educational and Psychological Measurement*, 70(5), 796-807.
- Allport, G. W. (1927). Concepts of trait and personality. *Psychological Bulletin*, 24(5), 284-293.
- Allport, G. W. (1961). *Pattern and growth in personality*. Oxford, England: Reinhart & Winston.
- Allport, G. W., & Ross, J. M. (1967). Personal religious orientation and prejudice. *Journal of Personality and Social Psychology*, 5(4), 432-443.
- Aristotle. (1999). *Nicomachean ethics* (T. Irwin, Trans). Indianapolis, IN: Hackett Publishing Company, Inc.
- Athanassoulis, N. (2010, July). Virtue Ethics. *The Internet Encyclopedia of Philosophy* Retrieved February 2, 2012, from <http://www.iep.utm.edu/virtue/>
- Audi, R. (Ed.). (2006). *The Cambridge dictionary of philosophy* (2nd ed.). New York, NY: Cambridge University Press.
- Baatard, G. (2012). A technical guide to effective and accessible web surveys *The Electronic Journal of Business Research Methods*, 10(2), 101-109.

- Babyak, M. A. (2004). What you see may not be what you get: A brief, nontechnical introduction to overfitting in regression-type models. *Psychosomatic Medicine*, 66(3), 411-421.
- Bandura, A. (1991a). Social cognitive theory of moral thought and action. In W. M. Kurtines & J. L. Gewirtz (Eds.), *Handbook of moral behavior and development (Vol. 1)* (pp. 2-46). Hillsdale, NJ: Lawrence Erlbaum Associates.
- Bandura, A. (1991b). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes*, 50(2), 248-287.
- Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review*, 3(3), 193-209.
- Bandura, A. (2006). Toward a psychology of human agency. *Perspectives on Psychological Science*, 1(2), 164-180.
- Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: A study of situational ethics. *MIS Quarterly*, 22(1), 31-60.
- Bartels, D. M. (2008). Principled moral sentiment and the flexibility of moral judgment and decision making. *Cognition*, 108(2), 381-417.
- Baykara, Z. G., Demir, S. G., & Yaman, S. (2014). The effect of ethics training on students recognizing ethical violations and developing moral sensitivity. *Nursing Ethics*(0969733014542673).
- Bebeau, M. J. (2002). The defining issues test and the four component model: Contributions to professional education. *Journal of Moral Education*, 31(3), 271-295.

- Bebeau, M. J. (2008). Promoting ethical development and professionalism: Insights from education research in the professions. *University of St. Thomas Law Journal*, 5(2), 366-403.
- Bebeau, M. J. (2009a). Enhancing professionalism using ethics education as part of a dental licensing board's disciplinary action: Part 1 An evidence-based process. *Journal of the American College of Dentists*, 76(2), 38-50.
- Bebeau, M. J. (2009b). Enhancing professionalism using ethics education as part of a dental licensing board's disciplinary action: Part 2 Evidence the process works. *Journal of the American College of Dentists*, 76(3), 32-45.
- Bebeau, M. J., & Monson, V. E. (2008). Guided by theory, grounded in evidence: A way forward for professional ethics education. In D. Narvaez & L. Nucci (Eds.), *Handbook on Moral and Character Education* (pp. 557-582). New York, NY: Taylor & Francis.
- Bebeau, M. J., & Monson, V. E. (2012). Professional identity formation and transformation across the life span. In A. McKee & M. Fraut (Eds.), *Innovation and change in professional education* (pp. 135-162). New York, NY: Springer.
- Bebeau, M. J., Rest, J. R., & Narvaez, D. (1999). Beyond the promise: A perspective on research in moral education. *Educational Researcher*, 28(4), 18-26.
- Bebeau, M. J., & Thoma, S. J. (1998). *Designing and testing a measure of intermediate level ethical concepts*. Paper presented at the Annual Meeting of the American Educational Research Association, San Diego, CA.
- Bebeau, M. J., & Thoma, S. J. (1999). "Intermediate" concepts and the connection to moral education. *Educational Psychology Review*, 11(4), 343-360.

- Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017-1041.
- Bennett, L., & Chenicheri, S. N. (2010). A recipe for effective participation rates for web-based surveys. *Assessment & Evaluation in Higher Education*, 35(4), 357-365.
- Bergman, R. (2002). Why be moral? A conceptual model from developmental psychology. *Human Development*, 45(2), 104-124.
- Bishop, D. A. (2006). To serve and protect: Do businesses have a legal duty to protect collections of personal information? *Shidler Journal of Law, Commerce, and Technology* Retrieved February 5, 2011, from <http://www.lctjournal.washington.edu/Vol3/a007Bishop.html>
- Blasi, A. (1980). Bridging cognition and moral action: A critical review of the literature. *Psychological Bulletin*, 88(1), 1-45.
- Blasi, A. (1983). Moral cognition and moral actions: A theoretical perspective. *Developmental Review*, 3(2), 178-210.
- Blasi, A. (1999). Emotions and moral motivation. *Journal for the Theory of Social Behavior*, 29(1), 1-19.
- Blasi, A. (2005). Moral character: A psychological approach. In D. K. Lapsley & F. C. Power (Eds.), *Character psychology and character education* (pp. 67-100). Notre Dame, IN: University of Notre Dame Press.
- Bommer, M., Gratto, C., J. G., & Tuttle, M. (1987). A behavioral model of ethical and unethical decision making. *Journal of Business Ethics*, 6(4), 265-280.
- Boudol, G. (2008). Secure information flow as a safety property. In P. Degano, J. Guttman & F. Martinelli (Eds.), *Formal Aspects in Security and Trust*: (pp. 20-30). Berlin, Germany: Springer Berlin Heidelberg.

- Bowern, M., Burmeister, O. K., Gotterbarn, D., & Weckert, J. (2006). ICT integrity: Bringing the ACS code of ethics up to date. *Australasian Journal of Information Systems, 13*(2), 169-182.
- Bricknell, K. I., & Cohen, J. F. (2005). Codes of ethics and the information technology employee: The impact of code institutionalization, awareness, understanding and enforcement. *Southern African Business Review, 9*(3), 54-65.
- Brief, A. P., & Motowidlo, S. J. (1986). Prosocial organizational behaviors *The Academy of Management Review, 11*(4), 710-725.
- Briggs, S. R., & Cheek, J. M. (1986). The role of factor analysis in the evaluation of personality scales. *Journal of Personality, 54*(1), 106-148.
- Brinkman, S. (2004). The topology of moral ecology. *Theory and Psychology, 14*(1), 57-80.
- Brooks, R. (2008). Addressing ethics and technology in business: Preparing today's students for the ethical challenges presented by technology in the workplace. *Contemporary Issues In Education Research, 1*(2), 23-32.
- Brown, M. E., Trevino, L. K., & Harrison, D. A. (2005). Ethical leadership: A social learning perspective for construct development and testing. *Organizational Behavior and Human Decision Processes, 97*(2), 117-134.
- Budeav, S. V. (2010). Using principal components and factor analysis in animal behaviour research: Caveats and guidelines. *Ethology, 116*(5), 472-480.
- Burchell, B., & Marsh, C. (1992). The effect of questionnaire length on survey response. *Quality & Quantity, 26*(3), 233-244.
- Bynum, T. W. (2001). Computer ethics: Its birth and its future. *Ethics and Information Technology, 3*(2), 109-112.

- Calo, R. M. (2011). The boundaries of privacy harm. *Indiana Law Journal*, 86(3), 1132-1161.
- Cannon, C. (2001). *Does education increase moral development? A re-examination of the moral reasoning abilities of working adult learners (Doctoral Dissertation)*. Nova Southeastern University, Fort Lauderdale, FL.
- Carlo, G., Hardy, S. A., & Alberts, M. (2006). Moral exemplars. In L. R. Sherrod, C. A. Flanagan, R. Kassimir & A. K. Syvertsen (Eds.), *Youth activism: An international encyclopedia* (Vol. 2, pp. 412-419). Westport, CT: Greenwood Press.
- Cattell, R. B. (1946). *Description and measurement of personality*. New York, NY: World Books.
- Cawley, M. J., Martin, J. E., & Johnson, J. A. (2000). A virtues approach to personality. *Personality and Individual Differences*, 28(5), 997-1003.
- Chafouleas, S. M., Christ, T. J., & Tiley-Tillman, T. C. (2009). Generalizability of scaling gradients on direct behavior ratings. *Educational and Psychological Measurement*, 69(1), 157-173.
- Chang, M. K. (1998). Predicting unethical behavior: A comparison of the theory of reasoned action and the theory of planned behavior. *Journal of Business Ethics*, 17(16), 1825-1834.
- Chatterjee, S., & Hadi, A. S. (1986). Influential observations, high leverage points, and outliers in regression. *I*, 3(379-393).
- Chiu, R. K. (2003). Ethical judgment and whistleblowing intention: Examining the moderating role of locus of control. *Journal of Business Ethics*, 43(1/2), 65-74.

- Chow, W. S. (2001). Ethical belief and behavior of managers using information technology for decision making in Hong Kong. *Journal of Managerial Psychology, 16*(4), 258-267.
- Christie, T., Groarke, L., & Sweet, W. (2008). Virtue ethics as an alternative to deontological and consequential reasoning in the harm reduction debate. *International Journal of Drug Policy, 19*(1), 52-58.
- Chung, H. M., & Khan, M. B. (2008). Classification of unethical behaviors in the management of information systems: The use of behaviorally anchored rating scale procedures. *International Journal of management, 25*(2), 262-269.
- Cohen, J. (1962). The statistical power of abnormal-social psychological research: A review. *Journal of Abnormal and Social Psychology, 65*(3), 145-153.
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2 ed.). Hillsdale, N.J.: Lawrence Erlbaum Associates.
- Colby, A., & Damon, W. (1992). *Some do care*. New York, NY: Macmillan, Inc.
- Cordoba, J. (2005, April). *Are we information systems professionals? A critical review*. Paper presented at the Young Operational Research Conference, Bath, England.
- Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology, 78*(1), 98-104.
- Courtenay, B. C., & Weidemann, C. (1985). The effects of a "don't know" response on Palmore's Facts on Aging quizzes. *The Gerontologist, 25*(2), 177-181.
- Cox, E. P. (1980). The optimal number of response alternatives for a scale: A review. *Journal of Marketing Research, 17*(4), 407-422.
- Creswell, J. W. (2012). *Educational Research: Planning, conducting, and evaluating quantitative and qualitative research* (4 ed.). Boston, MA: Pearson Education.

- Cronan, T. P., & Douglas, D. E. (2006). Toward a comprehensive ethical behavior model for information technology. *Journal of Organizational and End User Computing*, 18(1), 1-11.
- Cronan, T. P., & Douglas, D. E. (2008). A proposed IT ethical behavioral model. In S. Clarke (Ed.), *End user computing challenges and technologies: Emerging tools and applications* (pp. 1-12). Hershey, PA: IGI Global.
- Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297-334.
- Crowne, D. P., & Marlowe, D. (1960). A new scale of social desirability independent of psychopathology. *Journal of Consulting Psychology*, 24(4), 349-354.
- Cullen, J. B., Victor, B., & Stephens, C. (1989). An ethical weather report: Assessing the organization's ethical climate. *Organizational Dynamics*, 18(2), 50-62.
- Cyber-Ark. (2008a). *Survey Reveals Scandal of Snooping IT Staff* Retrieved September 10, 2009, from [http://www.nymity.com/Free\\_Privacy\\_Resources/Previews/ReferencePreview.aspx?guid=e07a0667-e140-4446-b24f-d8b3ec8f9150](http://www.nymity.com/Free_Privacy_Resources/Previews/ReferencePreview.aspx?guid=e07a0667-e140-4446-b24f-d8b3ec8f9150)
- Cyber-Ark. (2008b). *The global recession and its effect on work ethics* Retrieved September 10, 2009, from <http://www.cyber-ark.com/pdf/Ethics-Survey-Results.pdf>
- Cyber-Ark. (2009). *2009 Trust, security & passwords survey research brief* Retrieved September 15, 2009, from [http://www.cyber-ark.com/pdf/Cyber-Ark\\_Spring\\_2009\\_Snooping\\_Survey.pdf](http://www.cyber-ark.com/pdf/Cyber-Ark_Spring_2009_Snooping_Survey.pdf)
- Cyber-Ark. (2010). *Snooping survey* Retrieved August 10, 2010, from [http://www.cyber-ark.com/pdf/Cyber-Ark\\_2010\\_Snooping\\_Survey.pdf](http://www.cyber-ark.com/pdf/Cyber-Ark_2010_Snooping_Survey.pdf).



- Cyber-Ark. (2011). Cyber-Ark snooping survey Retrieved May 1, 2012, from <http://www.cyber-ark.com/downloads/pdf/2011-Snooping-Survey-data.pdf>
- Cyber-Ark. (2011). Cyber-Ark snooping survey Retrieved May 1, 2012, from <http://www.cyber-ark.com/downloads/pdf/2011-Snooping-Survey-data.pdf>
- Darwall, S. (1998). *Philosophical ethics*. Boulder, CO: Westview Press.
- Davis, L. L. (1992). Getting the most from a panel of experts. *Applied Nursing Research*, 5(4), 194-197.
- Davis, M. (2009). *Code making: How software engineering became a profession*. Illinois, IN: Center for the Study of Ethics in the Professions, Illinois Institute of Technology.
- Davison, R. M., Martinsons, M. G., Ou, C. X. J., Murata, K., Drummond, D., Li, Y., & H., L. H. W. (2009). The ethics of IT professionals in Japan and China. *Journal of the Association for Information systems*, 10(11), Article 1.
- De Maesschalck, R., Jouan-Rimbaud, D., & Massart, D. L. (2000). The Mahalanobis distance. *Chemometrics and intelligent laboratory systems*, 50(1), 1-18.
- De Raad, B., & Van Oudenhoven, J. P. (2011). A psycholexical study of virtues in the dutch language, and relations between virtues and personality. *European Journal of Personality*, 25(1), 43-52.
- Digman, J. M. (1990). Personality structure: Emergence of the five-factor model. *Annual Review of Psychology*, 41, 417-440.
- Dillman, D. (2000). *Mail and Internet surveys: The tailored design method*. New York, N.Y.: John Wiley & Sons, Inc.
- Donagan, A. (1977). *The theory of morality*. Chicago, IL: The University of Chicago Press.

- Dozier, J. B., & Miceli, M. P. (1985). Potential predictors of whistle-blowing: A prosocial behavior perspective. *Academy of Management Review*, *10*(4), 823-836.
- Dunlop, W. L., Walker, L. J., & Matsuba, M. K. (2012). The distinctive moral personality of care exemplars. *The Journal of Positive Psychology*, *7*(2), 131-143.
- Einolf, C. J. (2013). Daily spiritual experiences and prosocial behavior. *Social Indicators Research*, *110*(1), 71-87.
- Emerson, T. L. N., & Mckinney, J. A. (2010). Importance of religious beliefs to ethical attitudes in business. *Journal of religion and business ethics*, *1*(2), Article 5.
- Evans, J. R., & Mathur, A. (2005). The value of online surveys. *Internet Research*, *15*(2), 195-219.
- Eysenck, H. J. (1970). *The structure of human personality* (3rd ed.). London: Methuen.
- Flemming, C. M., & Bowden, M. (2009). Web-based surveys as an alternative to traditional mail methods. *Journal of Environmental Management*, *90*(1), 284-292.
- Freeman, W. J. (2007). *Moral maturity and the knowledge management firm (Doctoral Dissertation)*. Nova Southeastern University, Fort Lauderdale, FL.
- Freund, J. (2006). Technology student attitudes regarding privacy scenarios. In K. Elleithy, T. Sobh, A. Mahmood, M. Iskander & M. Karim (Eds.), *Advances in Computer, Information, and Systems Sciences, and Engineering: Proceedings of IETA 2005, TeNe 2005, EIAE 2005* (pp. 419-426). New York: Springer-Verlag.
- Friedman, H. H., Wilamowsky, Y., & Friedman, L. W. (1981). A comparison of balanced and unbalanced rating scales. *The Mid-Atlantic Journal of Business*, *19*(2), 1-7.
- Frimer, J. A., & Walker, L. J. (2008). Towards a new paradigm of moral personhood. *Journal of Moral Education*, *37*(3), 333-356.

- Frimer, J. A., Walker, L. J., Dunlop, W. L., Lee, B. H., & Riches, A. (2011). The integration of agency and communion in moral personality: Evidence of enlightened self-interest. *Journal of Personality and Social Psychology, 101*(1), 149-163.
- Frimer, J. A., Walker, L. J., Lee, B. H., Riches, A., & Dunlop, W. L. (2012). Hierarchical integration of agency and communion: A study of influential moral figures. *Journal of Personality, 80*(4), 1117-1145.
- Frisque, D., & Kolb, J. (2008). The effects of an ethics training program on attitude, knowledge, and transfer of training of office professionals: A treatment-and control-group design. *Journal of Human Resource Development Quarterly, 19*(1), 35-53.
- Fule, P., & Roddick, J. (2004). *Detecting privacy and ethical sensitivity in data mining results*. Paper presented at the Proceedings of the 27th Australasian Conference on Computer Science, Dunedin, New Zealand.
- Fuller, U., Keim, B., Fitch, D., Little, J. C., Riedesel, C., & White, S. (2009). Perspectives on developing and accessing professional values in computing. *ACM SIG on Computer Science Education, 41*(4), 174-194.
- Garland, R. (1991). The mid-point on a rating scale: Is it desirable? *Marketing Bulletin, 2*(3), 1-4.
- Ghosh, S., & Turrini, E. (2010). *Cybercrimes: A multidisciplinary analysis*. Heidelberg, Germany: Springer-Verlag.
- Gilligan, C. (1982). *In a different voice: Psychological theory and women's development*. Cambridge, MA: Harvard University Press.

- Gleason, D. H. (2003). *ICT professionalism*. Paper presented at the ETICOMP, Lisbon, Portugal.
- Gorsuch, R. L. (1983). *Factor analysis (2nd. Ed.)*. Hillsdale, NJ: Erlbaum.
- Gotsis, G., & Kortezi, Z. (2007). Philosophical foundations of workplace spirituality: A critical approach. *Journal of Business Ethics, 78*(4), 575-600.
- Grady, C., Danis, M., Soeken, K. L., O'Donnell, P., Taylor, C., Farrar, A., & Ulrich, C. M. (2008). Does ethics education influence the moral action of practicing nurses and social workers? *The American Journal of Bioethics, 8*(4), 4-11.
- Green, S. B. (1991). How many subjects does it take to do a regression analysis? *Multivariate Behavioral Research, 26*(3), 499-510.
- Greenlaw, C., & Brown-Welty, S. (2009). A Comparison of Web-Based and Paper-Based Survey Methods : Testing Assumptions of Survey Mode and Response Cost. *Evaluation Review, 33*(5), 464-480.
- Haines, R., & Leonard, L. N. K. (2007). Individual characteristics and ethical decision-making in an IT context. *Industrial Management & Data Systems, 107*(1), 5-20.
- Hamilton, N. W., & Monson, V. (2012). Legal education's ethical challenge: Empirical research on how most effectively to foster each student's professional formation (Professionalism). *University of St. Thomas Law Journal, 9*(2), 325-402.
- Hannah, S. T., Avokio, B. J., & Walumbwa, F. O. (2011). Relationships between authentic leadership, moral courage, and ethical and pro-social behaviors. *Business Ethics Quarterly, 21*(4), 555-578.
- Hardy, S. A. (2006). Identity, reasoning, and emotion: An empirical comparison of three sources of moral motivation. *Motivation and Emotion, 30*(3), 205-213.

- Hardy, S. A., & Carlo, G. (2005a). Identity as a source of moral motivation. *Human Development, 48*(4), 232-256.
- Hardy, S. A., & Carlo, G. (2005b). Religiosity and prosocial behaviours in adolescence: The mediating role of prosocial values. *Journal of Moral Education, 34*(2), 231-249.
- Hardy, S. A., & Carlo, G. (2011a). Moral identity: What is it, how does it develop, and is it linked to moral action? *Child Development, 5*(3), 212-218.
- Hardy, S. A., & Carlo, G. (2011b). Moral Identity. In S. J. Schwartz, K. Luyckx & V. L. Vignoles (Eds.), *Handbook of Identity Theory and Research, Volume 1: Structures and processes* (Vol. 1, pp. 495-513). New York, NY: Springer.
- Hardy, S. A., Walker, L. J., Rackham, D. D., & Olsen, J. A. (2012). Religiosity and adolescent empathy and aggression: The mediating role of moral identity. *Psychology of Religion and Spirituality, 4*(3), 237-248.
- Harrington, S. J. (1996). The effects of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257-278.
- Harrington, S. J., & McCollum, R. L. (1990). Lessons from corporate America applied to training in computer ethics. *ACM Special Interest Group on Security, Audit, and Control, 8*(3), 23-28.
- Hartshorne, J. (2010). The value of privacy. *Journal of Media Law, 2*(1), 67-84.
- Helms, J. E., Henze, K. T., Sass, T. L., & Mifsud, V. A. (2006). Treating cronbach's alpha reliability coefficients as data in counseling research. *the Counseling Psychologist, 34*(5), 630-660.

- Henson, R. K., & Roberts, J. K. (2006). Use of exploratory factor analysis in published research: Common errors and some comment on improved practice. *Educational and Psychological Measurement, 66*(3), 393-416.
- Hill, J. (2009). Probabilism today: Permissibility and multi-account ethics. *Australasian Journal of Philosophy 87*(2), 235-250.
- Himma, K. E., & Tavani, H. T. (Ed.). (2008). *The handbook of information and computer ethics*. Hoboken, NJ: John Wiley & Sons, Inc.
- Holtzman, D. H. (2006). *Privacy lost: How technology is endangering your privacy*. San Francisco, CA: Jossey-Bass Books.
- Hovorka, D. S., Germonprez, M., & Larsen, K. R. (2008). Explanation in information systems. *Information Systems Journal, 18*(1), 23-43.
- Huff, C. (2008). It is not all straw, but it can catch fire: In defense of impossible ideals in computing - A comment on "a critique of positive responsibility in computing". *Science and Engineering Ethics, 14*(2), 241-244.
- Huff, C. (2011). What does knowledge have to do with ethics? In G. J. M. d. Costa (Ed.), *Ethical issues and social dilemmas in knowledge management: Organizational innovation* (pp. 17-27). Hershey, PA: IGI Global.
- Huff, C., & Barnard, L. (2009). Good computing: Moral exemplars in the computing profession. *IEEE Technology and Society Magazine, 28*(3), 47-57.
- Huff, C., Barnard, L., & Frey, W. (2008a). Good computing: A pedagogically focused model of virtue in the practice of computing (part 1). *Journal of Information, Communication & Ethics in Society, 6*(3), 246-278.

- Huff, C., Barnard, L., & Frey, W. (2008b). Good computing: A pedagogically focused model of virtue in the practice of computing (part 2). *Journal of Information, Communication & Ethics in Society*, 6(4), 284-316.
- Huff, C., & Frey, W. (2005). Moral pedagogy and practical ethics. *Science and Engineering Ethics*, 11(3), 389-408.
- Huff, C., Gaasedelen, O., Baker, C., Irvin, J., & Payne, C. (2011). *Making Sense of Moral Failings in Moral Exemplars*. Paper presented at the Computer Ethics Philosophical Enquiry, Milwaukee, WI. Abstract retrieved from <http://users.gw.utwente.nl/Coeckelbergh/site/publicaties/Conference%20Proceedings.pdf>
- Huff, C., & Hughes, K. (2012). Moral Exemplars. In W. S. Bainbridge (Ed.), *Leadership in science and technology: A reference handbook* (pp. 249-254). Thousand Oaks, CA: SAGE Publications.
- Huff, C., & Rogerson, S. (2005, September). *Craft and reform in moral exemplars in computing* Paper presented at the ETHICOMP, Linkoping, Sweden.
- Hursthouse, R. (1999). *On virtue ethics*. New York, NY: Oxford University Press.
- Ishida, C. (2006). How do scores of DIT and MJT differ? A critical assessment of the use of alternative moral development scales in studies of business ethics. *Journal of Business Ethics*, 67(1), 63-74.
- Jamieson, R., Land, L., Sarre, R., Steel, A., Stephens, G., & Winchester, D. (2008, December). *Defining identity crimes*. Paper presented at the 19th Australasian Conference on Information Systems, Christchurch, New Zealand.

- Jeffries, V., Johnston, B. V., Nichols, L. T., Oliner, S. P., Tiryakian, E., & Weinstein, J. (2006). Altruism and social solidarity: Envisioning a field of specialization. *American Sociologist*, 37(3), 67-83.
- Jin, K. G., & Drozdenko, R. (2003). Manager's perceived organizational values and ethical attitudes in the direct marketing industry. *Business and Professional Ethics Journal*, 22(4), 43-66.
- Jin, K. G., Drozdenko, R., & Bassett, R. (2007). Information technology professionals' perceived organizational values and managerial ethics: An empirical study. *Journal of Business Ethics*, 71(2), 149-159.
- Jin, K. G., Drozdenko, R., & Deloughy, S. (2010). *An empirical investigation of the existence of organizational typologies*. Paper presented at the Proceedings of the American Society of Business and Behavioral Sciences, Las Vegas, NV.
- Jin, K. G., & Drozdenko, R. G. (2010). Relationships among perceived organizational core values, corporate social responsibility, ethics, and organizational performance outcomes: An empirical study of information technology professionals. *Journal of Business Ethics*, 93(3), 341-359.
- John, O. P., Naumann, L. P., & Soto, C. J. (2008). Paradigm shift to the integrative big five taxonomy: History, measurement, and conceptual issues. In O. P. John, R. W. Robins & L. A. Pervin (Eds.), *Handbook of personality: Theory and research 3rd ed.* (pp. 114-158). New York, NY: Guilford Press.
- Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, 33(7), 14-26.
- Kalton, G., Roberts, J. A., & Holt, D. (2009). The effects of offering a middle response option with option questions. *The Statistician*, 29(1), 65-78.



- Kaptein, M. (2011). Towards effective codes: Testing the relationship with unethical behavior. *Journal of Business Ethics*, 99(2), 233-251.
- Kaptein, M., & Schwartz, M. S. (2008). The effectiveness of business codes: A critical examination of existing studies and the development of an integrated research model. *Journal of Business Ethics*, 77(2), 111-127.
- Karjalainen, M., & Siponen, M. (2011). Towards a new meta-theory of designing information systems (IS) training approaches. *Journal of the Association for Information Systems*, 12(8), 518-555.
- Keefer, M., & Ashley, K. D. (2001). Case-based approaches to professional ethics: A systematic comparison of students' and ethicists moral reasoning. *Journal of Moral Education*, 30(4), 377-398.
- Keefer, M. W. (2005). Making good use of online case study material. *Science and Engineering Ethics*, 11(3), 413-429.
- Kim, C. (1996). Cook's distance in spline smoothing. *Statistics & Probability Letters*, 31(2), 139-144.
- Kohlberg, L. (1969). Stage and sequence: The cognitive developmental approach to socialization. In D. A. Goslin (Ed.), *Handbook of socialization theory* (pp. 347-480). Chicago, IL: Rand McNally.
- Kohlberg, L. (1984). *Essays on moral development: The psychology of moral development (Vol. 2), The nature and validity of moral stages*. San Francisco, CA: HarperCollins.
- Komorita, S. S. (1963). Attitude content, intensity and the neutral point on a Likert scale. *Journal of Social Psychology*, 61(2), 327-334.

- Krishnamurthy, B., & Wills, C. E. (2010). On the leakage of personally identifiable information via online social networks. *ACM Special Interest Group Computer Communication Review, 40*(1), 112-117.
- Kuijpers, R. E., van der Ark, L. A., & Croon, M. A. (2013). Testing hypotheses involving Cronbach's alpha using marginal models. *British Journal of Mathematical and Statistical Psychology, 66*(3), 503-520.
- Kuo, F. Y., Lin, C. S., & Hsu, M. H. (2007). Assessing gender differences in computer professionals' self-regulatory efficacy concerning information privacy practices. *Journal of Business Ethics, 73*(2), 145-160.
- Kuzu, A. (2009). Problems related to computer ethics: Origins of the problems and suggested solutions. *The Turkish Online Journal of Educational Technology, 8*(2), 91-110.
- Lapsley, D. K., & Hill, P. L. (2009). The development of the moral personality. In D. Narvaez & D. K. Lapsley (Eds.), *Personality, identity, and character: Explorations in moral psychology* (Vol. 185-213). New York, NY: Cambridge University Press.
- Lapsley, D. K., & Narvaez, D. (2006). Character education. In K. A. Renninger & I. E. Sigel (Eds.), *Handbook of child psychology* (Vol. 6, pp. 248-296). Hoboken, NJ: John Wiley & Sons.
- Leonard, L. N. K., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions - planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management, 42*(1), 143-158.

- Leonard, L. N. K., & Cronan, T. P. (2001). Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. *Journal of the Association for Information Systems*, 1(1), Article 12.
- Leonard, L. N. K., & Cronan, T. P. (2005). Attitude toward ethical behavior in computer use: A shifting model. *Industrial Management & Data systems*, 105(9), 1150-1171.
- Lever, A. (2008). Mrs. Aremac and the camera: A response to Ryber. *Res Publica: A Journal of Moral, Legal, and Social Philosophy*, 14(1), 35-42.
- Liao, D., & Valliant, R. (2012). Variance inflation factors in the analysis of complex survey data. *Survey Methodology*, 38(1), 53-62.
- Lietz, P. (2008). Questionnaire design in attitude and opinion research: Current state of an art: Jacobs University Bremen.
- Lincoln, S. H., & Holmes, E. K. (2011). Ethical decision making: A process influenced by moral intensity. *Journal of Healthcare, Science and the Humanities*, 1(1), 55-69.
- Linderman, J. L., & Schiano, W. T. (2001). Information ethics in a responsibility vacuum. *The DATA BASE for Advances in Information Systems*, 32(1), 70-74.
- Little, J. C., Granger, M. J., Boyle, R., Gerthardt-Powals, J., Impagliazzo, J., Janik, C., . . . Soja, P. (1999). Integrating professionalism and workplace issues into the computing and information technology curriculum: Report of the annual conference on innovation and technology in computer science education ITiCSE'99 working group on professionalism. *ACM SIG on Computer Science Education*, 31(4), 106-120.

- Lucas, R. E., & Donnellan, M. B. (2009). Age differences in personality: Evidence from a nationally representative Australian sample. *Developmental Psychology, 45*(5), 1353-1363.
- Macfarlane, B. (2010). Values and virtues in qualitative research. In M. Savin-Baden & C. H. Major (Eds.), *New approaches to qualitative research: Wisdom and uncertainty* (pp. 19-27). New York, NY: Routledge.
- Maclean, A. M., Walker, L. J., & Matsuba, M. K. (2004). Transcendence and the Moral Self: Identity integration, religion, and moral life. *Journal for the Scientific Study of Religion, 43*(3), 429-437.
- Martin, N. L., & Woodward, B. S. (2011). Computer ethics of American and European information technology students: A cross-cultural comparison. *Issues in Information Systems, 12*(1), 78-87.
- Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly, 10*(1), 4-12.
- Mastain, L. (2007). A phenomenological investigation of altruism as experienced by moral exemplars. *Journal of Phenomenological Psychology, 38*(1), 62-99.
- Matell, M. S., & Jacoby, J. (1972). Is there an optimal number of alternatives for Likert scale items? Effects of testing time and scale properties. *Journal of Applied Psychology, 56*(6), 506-509.
- Matsuba, M. K., & Walker, L. J. (2004). Extraordinary moral commitment: Young adults involved in social organizations. *Journal of Personality, 72*(2), 413-436.
- Matsuba, M. K., & Walker, L. J. (2005). Young adult moral exemplars: The making of self through stories. *Journal of Research on Adolescence, 15*(3), 275-297.

- Maxwell, S. E. (2004). The persistence of underpowered studies in psychological research: Causes, consequences, and remedies. *Psychological Methods, 9*(2), 147-163.
- McAdams, D. P. (2006). The redemptive self: Generativity and the stories Americans live by. *Research in Human Development, 3*(2&3), 81-100.
- McAdams, D. P., Albaugh, M., Farber, E., Daniels, J., Logan, R. L., & Olson, B. (2008). Family metaphors and moral intuitions: How conservative and liberals narrate their lives. *Journal of Personality and Social Psychology, 95*(4), 978-990.
- McAdams, D. P., & Pals, J. L. (2006). A new big five: Fundamental principles for an integrative science of personality. *American Psychologist, 61*(3), 204-217.
- McCallister, E., Garance, T., & Scarfone, K. (2010). *Guide to protecting the confidentiality of personally identifiable information (PII): Recommendations of the National Institute of Standards and Technology*. (NIST Special Publication 800-122). Gaithersburg, MD: National Institute of Standards and Technology.
- Messmer, E. (2009). Survey: 59 percent of fired workers would steal data on the way out Retrieved April 6, 2009, from <http://www.itworld.com/business/63080/survey-59-percent-fired-workers-steal-data-way-out>
- Miceli, M. P., Near, J. P., Rehg, M. T., & Van Scotter, J. R. (2012). Predicting employee reactions to perceived organizational wrongdoing: Demoralization, justice, proactive personality, and whistle-blowing. *Human Relations, 65*(8), 923-954.
- Miller, M. L., & Schlenker, B. R. (2011). Integrity and identity: Moral identity differences and preferred interpersonal relations. *European Journal of Personality, 25*(1), 2-15.

- Mobely, S. E. F. (2002). *The study of Lawrence Kohlberg's stages of moral development theory and ethics: Considerations in public administration practices* (Doctoral Dissertation). Nova Southeastern University, Ft. Lauderdale, FL.
- Moberg, D. J. (2000). Role models and moral exemplars: How do employees acquire virtues by observing others? *Business Ethics Quarterly*, 10(3), 675-696.
- Monson, V. (2009). *Moral judgment, role concepts, and empathic response as predictors of dental student clinical effectiveness*. (Doctoral Dissertation) University of Minnesota.
- Moor, J. H. (1990). Ethics of privacy protection. *Library Trends*, 39(1 & 2), 69-82.
- Moor, J. H. (1997). Towards a theory of privacy in the information age. *Computers and Society*, 27(3), 27-32.
- Mujataba, B. G., Cavico, F. J., McCartney, T. O., & DiPaolo, P. T. (2009). Ethics and retail management professionals: An examination of age, education, and experience variables. *American Journal of Business Education*, 2(3), 13-25.
- Mujataba, B. G., Cavico, F. J., & Sungkhawan, J. (2011). Business ethics of government employees and future lawyers in Thailand: A study of age, gender, management experience, and education. *International Business Research*, 4(1), 16-27.
- Mundry, R., & Nunn, C. L. (2009). Stepwise model fitting and statistical inference: Turning noise into signal pollution. *American Naturalist*, 173(1), 119-123.
- Muraven, M., & Baumeister, R. F. (2000). Self-regulation and depletion of limited resources: Does self-control resemble a muscle? *Psychological Bulletin*, 126(2), 247-259.

- Murphy, P. E. (1999). Character and virtue ethics in international marketing: An agenda for managers, researchers, and educators'. *Journal of Business Ethics*, 18(1), 107-125.
- Myyry, L. (2003). *Components of morality: A professional ethics perspective on moral motivation, moral sensitivity, moral reasoning and related constructs among university students*. (Doctoral Dissertation). University of Helsinki, Helsinki, Finland.
- Namlu, A. G., & Odabasi, H. F. (2007). Unethical computer using behavior scale: A study of reliability and validity on Turkish university students. *Computers & Education*, 48(2), 205-215.
- Narvaez, D. (2005). The neo-Kohlbergian tradition and beyond: Schemas, expertise, and character. In C. P. Edwards & G. Carlo (Eds.), *Nebraska Symposium on Motivation, Vol. 51: Moral Motivation through the Lifespan* (pp. 119-163). Lincoln, NE: University of Nebraska Press.
- Narvaez, D. (2006). Integrative ethical education. In M. Killen & J. G. Smetana (Eds.), *Handbook of moral development* (pp. 703-732). Mahwah, NJ: Lawrence Erlbaum Associates.
- Narvaez, D. (2008). Human flourishing and moral development: Cognitive and neurobiological perspectives of virtue development. In L. P. Nucci & D. Narvaez (Eds.), *Handbook of Moral and Character Education* (pp. 310-327). New York, NY: Routledge.
- Narvaez, D., Bock, T., Endicott, L., & Lies, J. M. (2004). Minnesota's community voices and character education project. *Journal of Research in Character Education*, 2(2), 89-112.

- Narvaez, D., & Lapsley, D. K. (2005). The psychological foundations of everyday morality and moral expertise. In D. K. Lapsley & E. C. Power (Eds.), *Character psychology and character education* (pp. 140-165). Notre Dame, IN: University of Notre Dame Press.
- Narvaez, D., & Lapsley, D. K. (Eds.). (2009a). *Personality, identity, and character: Explorations in moral psychology*. New York, NY: Cambridge University Press.
- Narvaez, D., & Lapsley, D. K. (2009b). Moral identity, moral functioning, and the development of moral character. In D. Bartels, C. Bauman, L. Skitka, D. L. Medin & B. H. Ross (Eds.), *Moral judgment and decision making (Psychology of learning & Motivation, Volume 50)* (Vol. 50, pp. 237-274). San Diego, CA: Academic Press.
- Neal, D. T., Wood, W., & Quinn, J. M. (2006). Habits – a repeat performance. *Current Directions in Psychological Science*, 15(4), 198-2002.
- Newman, G. R., & McNally, M. M. (2005). *Identity theft literature review*. Washington, DC: (NIJ Contract No. 2005-TO-008) Retrieved October 15, 2009, from <http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf>
- Niemiec, R. M. (2013). VIA character strengths: Research and practice (The first 10 years). In H. H. Koop & A. D. Fave (Eds.), *Cross-cultural advancements in positive psychology* (pp. 11-29). New York, NY: Springer.
- Nisigandha, B. (2007). The role of character in ethical decision-making. *The Journal of Value Inquiry*, 41(1), 45-57.
- Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy*, 17(5-6), 559-596.



- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law review*, 79(119), 101-139.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory*, 3rd ed. New York, NY: McGraw-Hill.
- O'Boyle, E. J. (2002). An ethical decision-making process for computing professionals. *Ethics and Information Technology*, 4(4), 267-277.
- O'Brian, R. M. (2007). A caution regarding rules of thumb for variance inflation factors. *Quality & Quantity*, 41(5), 673-690.
- Oliner, S. P., & Oliner, P. M. (1988). *The altruistic personality: Rescuers of Jews in Nazi Europe*. New York, NY: Free Press.
- Osborne, J. W., & Costello, A. B. (2004). Sample size and subject to item ratio in principal components analysis. *Practical Assessment, Research & Evaluation*, 9(11). Retrieved from <http://PAREonline.net/getvn.asp?v=9&n=11>
- Oz, E. (1992). Ethical standards for information systems professionals: A case for a unified code. *MIS Quarterly*, 16(4), 423-433.
- Oz, E. (1993). Ethical standards for computer professionals: A comparative analysis of four major codes. *Journal of Business Ethics*, 12(9), 709-726.
- Pan, Y., & Jackson, R. T. (2008). Ethnic difference in the relationship between acute inflammation and serum ferritin in US adult males. *Epidemiology and Infection*, 136(3), 421-431.
- Parboteeah, K. P., Hogel, M., & Cullen, J. B. (2007). Ethics and religion: An empirical test of a multidimensional model. *Journal of Business Ethics*, 80(2), 387-398.

- Parker, D. B. (1968). Rules of ethics in information processing. *Communications of the ACM*, 11(3), 198-201.
- Penner, L. A., Fritzsche, B. A., Craiger, J. P., & Freifeld, T. R. (1995). Measuring the prosocial personality. In J. Butcher & C. D. Spielberger (Eds.), *Advances in personality assessment* (pp. 147-184). New York, NY: Lawrence Erlbaum Associates, Inc.
- Penny, K. L. (1996). Appropriate critical values when testing for a single multivariate outlier by using the mahalanobis distance. *Journal of the Royal Statistical Society. Series C (Applied Statistics)*, 45(1), 73-81.
- Peslak, A. R. (2006). An exploratory investigation of information technology ethics factors. *Issues in Information Systems*, 7(2), 339-343.
- Peslak, A. R. (2007, September 10). Ethics and moral intensity: An analysis of information technology and general education students. *Information Systems Education Journal*, 5(26), 1-12. Retrieved from [http://www.isedj.org/5/26/ISEDJ.5\(26\).Peslak.pdf](http://www.isedj.org/5/26/ISEDJ.5(26).Peslak.pdf)
- Peterson, C., & Seligman, M. E. (2004). *Character strengths and virtues: A handbook and classification*. New York, NY: Oxford University Press.
- Piaget, J. (1932). *The moral judgment of the child*. London: Routledge & Kegan Paul.
- Plaisance, P. L. (2011). Moral agency in media: Toward a model to explore key components of ethical practice. *Journal of Mass Media Ethics: Exploring Questions of Media Morality* 26(2), 96-113.
- Porter, S. R. (2004). Raising response rates: What works? *Overcoming Survey Research Problems*, 2004(121), 5-21.

- Post, R. C. (2001). Three concepts of privacy. *Yale Law School Faculty Scholarship Series*, (Paper 185). Retrieved from [http://digitalcommons.law.yale.edu/fss\\_papers/185](http://digitalcommons.law.yale.edu/fss_papers/185)
- Power, E. M. (2007). Developing a culture of privacy: A case study. *IEEE Security & Privacy*, 5(6), 58-60.
- Preacher, K. J., & MacCallum, R. C. (2002). Exploratory factor analysis in behavior genetics research: Factor recovery with small sample sizes. *Behavior Genetics*, 32(2), 153-161.
- Preston, C. C., & Colman, A. M. (2000). Optimal number of response categories in rating scales: Reliability, validity, discriminating power, and respondent preferences. *Acta Psychologica*, 104(1), 1-15.
- Prior, M., Rogerson, S., & Fairweather, B. (2002). The ethical attitudes of information systems professionals: Outcomes of an initial survey. *Telematics and Informatics*, 19(1), 21-36.
- Pritchard, M. S. (1998). Professional responsibility focusing on the exemplary. *Science and Engineering Ethics*, 4(2), 215-233.
- Puhakainen, P. (2006). *A design theory for information security awareness (Doctoral Dissertation)*. University of Oulu, Finland. (Retrieved from <http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf>)
- Quallen, N. M. (2009). Recent development: Damages under the privacy act: Is emotional harm "actual". *North Carolina Law Review*, 88(1), 1-28.
- Reed, A., & Aquino, K. F. (2003). Moral identity and the expanding circle of moral regard towards out-groups. *Journal of Personality and Social Psychology*, 84(6), 1270-1286.

- Rest, J. (1983). Morality. In J. H. Flavell, E. M. Markman & P. Mussen (Eds.), *Handbook of child psychology (4th ed., Vol. 3)* (pp. 556-629). New York, NY: John Wiley and Sons.
- Rest, J. (1984). The major components of morality. In W. Kurtines & J. Gewitz (Eds.), *Morality, moral behavior, and moral development* (pp. 24-40). New York, NY: Wiley and Sons.
- Rest, J. (1986). *Moral development: Advances in research and theory*. New York, NY: Praeger.
- Rest, J., Thoma, S., & Edwards, L. (1997). Designing and validating a measure of moral judgment: Stage preference and stage consistency approaches. *Journal of Educational Psychology*, 89(1), 5-28.
- Rest, J., Thoma, S., Narvaez, D., & Bebeau, M. J. (1997). Alchemy and beyond: Indexing the defining issues test. *Journal of Educational Psychology*, 89(3), 498-507.
- Rest, J. R. (1975). Longitudinal study of the defining issues test of moral judgment: A strategy for analyzing developmental change. *Developmental Psychology*, 11(6), 738-748.
- Rest, J. R. (1979). *Development in judging moral issues*. Minneapolis, MN: University of Minnesota Press.
- Rest, J. R., Davison, M. L., & Robbins, S. (1978). Age trends in judging moral issues: A review of cross-sectional, longitudinal, and sequential studies of the Defining Issues Test. *Child Development*, 49(2), 263-279.
- Rest, J. R., & Narvaez, D. (1994). *Moral development in the professions: Psychology and applied ethics*. Hillsdale, NJ: Lawrence Erlbaum Associates.

- Rest, J. R., Narvaez, D., Thoma, S. J., & Bebeau, M. J. (1999). DIT2: Devising and testing a revised instrument of moral judgment. *Journal of Educational Psychology, 91*(4), 644-659.
- Rest, J. R., Narvaez, D., Thoma, S. J., & Bebeau, M. J. (2000). A neo-Kohlbergian approach to morality research. *Journal of Educational Psychology, 29*(4), 381-395.
- Reynolds, S. J. (2006). Moral awareness and ethical predispositions: Investigating the role of individual differences in the recognition of moral issues. *Journal of Applied Psychology, 91*(1), 233-243.
- Richardson, F. C. (2012). On psychology and virtue ethics. *Journal of Theoretical and Philosophical Psychology, 32*(1), 24-34.
- Roberts, B. W., & Mroczek, D. (2008). Personality trait change in adulthood. *Current Directions in Psychological Science, 17*(1), 31-35.
- Roberts, B. W., Walton, K. E., & Viechtbauer, W. (2006). Patterns of mean-level change in personality traits across the life course: A meta-analysis of longitudinal studies. *Psychological Bulletin, 132*(1), 1-25.
- Rodriguez-Dominguez, L., Gallego-Alvarez, I., & Garcia-Sanchez, I. M. (2009). Corporate governance and codes of ethics. *Journal of Business Ethics, 90*(2), 187-202.
- Romanosky, S., & Acquisti, A. (2009). Privacy costs and personal data protection: Economic and legal perspectives. *Berkely Technology Law Journal, 24*(3), 1062-1091.
- Rule, J. T., & Bebeau, M. J. (2005). *Dentists who care: Inspiring stories of professional commitment*. Hanover Park, IL: Quintessence Publishing Company.

- Ryan, J. A. (1998). Moral philosophy and moral psychology in Mencius. *Asian Philosophy*, 8(1), 47-64.
- Saia, R. (1998, March 16). "What would you do?: Ethical dilemmas and ethical decisions". *Computerworld*, 64-65.
- Schlenker, B. R., Miller, M. L., & Johnson, R. M. (2009). Moral identity, integrity, and personal responsibility. In D. Narvaez & D. Lapsley (Eds.), *Personality, identity, and character: Explorations in moral psychology* (pp. 316-340). New York, NY: Cambridge University Press.
- Sekerka, L. E. (2009). Organizational ethics education and training: A review of best practices and their application. *International Journal of Training and Development*, 13(2), 77-95.
- Shanahan, K. J., & Hyman, M. R. (2003). The development of a virtue ethics scale. *Journal of Business Ethics*, 42(2), 197-207.
- Shao, R., Aquino, K., & Freeman, D. (2008). Beyond moral reasoning: A review of moral identity research and its implications for business ethics. *Business Ethics Quarterly*, 18(4), 513-540.
- Shaw, E. D., Ruby, K. G., & Post, J. M. (1998). The insider threat to information systems. *Security Awareness Bulletin*, 2, 1-10.
- Singer, P. (2008). *Practical ethics* (2nd ed.). New York, NY: Cambridge University Press.
- Smith, G. (2009). Data mining: How hackers steal sensitive electronic information. *The Journal of Corporate Accounting & Finance*, 20(4), 23-26.
- Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review*, 53(6), 1393-1462.

- Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, 90(4), 1087-1155.
- Solove, D. J. (2003). Identity theft, privacy, and the architecture of vulnerability. *Hastings Law Journal*, 54(4), 1227-1276.
- Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 447-560.
- Solove, D. J. (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.
- Stahl, B. C. (2004). Responsibility for information assurance and privacy: A problem of individual ethics? *Journal of Organizational and End User Computing*, 16(3), 59-77.
- Stahl, B. C., & Wood, C. (2007). Forming IT professionals in the Internet age: A critical case study. In P. Yoong & S. Huff (Eds.), *Managing IT professionals in the Internet age*. Hershey, PA: Idea Group Publishing.
- Stevens, J. M., Steensma, H. K., Harrison, D. A., & Cochran, P. L. (2004). Symbolic or substantive document? The influence of ethics codes on financial executives' decisions. *Strategic Management Journal*, 26(2), 181-195.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 13(2), 147-169.
- Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, 2, 53-55.
- Tavani, H. T. (2005). Search engines, personal information and the problem of privacy in public. *International Review of Information Ethics*, 3(3), 40-45.
- Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *Computers and Society*, 31(1), 6-11.

- Telfer, E. (1990). The utility of the moral virtues in Aristotle's "Nicomachean Ethics". *Proceedings of the Aristotelian Society*, 90(1), 35-48.
- Thoma, S. J. (2006). Research on the Defining Issues Test. In M. Killen & J. G. Smetana (Eds.), *Handbook of moral development* (pp. 67-91). Mahwah, NJ: Lawrence Erlbaum Associates Publishers.
- Thoma, S. J., & Bebeau, M. J. (2013). Moral motivation and the four component model. In K. Heinrichs, F. Oser & T. Lovat (Eds.), *Handbook of moral motivation: Theories, models, applications* (pp. 49-67). The Netherlands: Sense Publishers.
- Trevino, L. K. (1986). Ethical decision making in organizations: A person-situation interactionist model. *The Academy of Management Review*, 11(3), 601-617.
- Trevino, L. K., & Brown, M. E. (2004). Managing to be ethical: Debunking five business ethics myths. *Academy of Management Executive*, 18(2), 69-81.
- Trevino, L. K., Weaver, G. R., & Reynolds, S. J. (2006). Behavioral ethics in organizations: A review. *Journal of Management*, 32(6), 951-990.
- Tsang, K. K. (2011). The use of midpoint on Likert scale: the implications for educational research. *Hong Kong Teachers' Centre Journal* Retrieved January 23, 2014, from [http://edb.org.hk/HKTC/download/journal/j11/HKTCJv11\\_11-B02.pdf](http://edb.org.hk/HKTC/download/journal/j11/HKTCJv11_11-B02.pdf)
- van den Hoven, J. (2008). Information technology, privacy, and the protection of personal data. In J. V. D. Hoven & J. Weckert (Eds.), *Information technology and moral philosophy* (pp. 301-321). New York, NY: Cambridge University Press.
- van Dierendonck, D. (2010). Servant leadership: A review and synthesis. *Journal of Management*, 20(10), 1-34.
- Van Selm, M., & Jankowski, N. W. (2006). Conducting online surveys. *Quality & Quantity*, 40(3), 435-456.



- van Wel, L., & Royakkers, L. (2004). Ethical issues in web data mining. *Ethics and Information Technology*, 6(2), 129-140.
- van Zyl, L. (2009). Agent-based virtue ethics and the problem of action guidance. *Journal of Moral Philosophy*, 6(1), 50-69.
- Victor, B., & Cullen, J. B. (1988). The organizational bases of ethical work climates. *Administrative Science Quarterly*, 33(1), 101-125.
- Vittinghoff, E., & McCulloch, C. E. (2007). Relaxing the rule of ten events per variable in logistic and Cox regression. *American Journal of Epidemiology*, 165(6), 710-718.
- Volkman, R. (2004, April 14-16). *Being a good computer professional: The advantages of virtue ethics in computing*. Paper presented at the Ethicomp, Syros, Greece.  
<http://www.ccsr.cse.dmu.ac.uk/conferences/ethicomp/ethicomp2004/abstracts/85.html>
- Waldo, J., Lin, H. S., & Millett, L. I. (2010). Thinking about privacy: Chapter 1 of "Engaging privacy and information technology in a digital age". *Journal of Privacy and Confidentiality*, 2(1), 19-50.
- Walker, A. G., Smither, J. W., & DeBode, J. (2011). The effects of religiosity on ethical judgments. *Journal of Business Ethics*, 106(4), 437-452.
- Walker, L. J. (1986). Experiential and cognitive sources of moral development in adulthood. *Human Development*, 29(2), 113-124.
- Walker, L. J. (1999). The perceived personality of moral exemplars. *Journal of Moral Education*, 28(2), 145-162.
- Walker, L. J. (2002a). The model and the measure: An appraisal of the Minnesota approach to moral development. *Journal of Moral Education*, 31(3), 353-367.

- Walker, L. J. (2002b). The character of moral exemplars Retrieved March 5, 2011, from <http://www.ed.gov/admins/lead/safety/character/walker.doc>
- Walker, L. J. (2003). Morality, religion, spirituality - the value of saintliness. *Journal of Moral Education*, 32(4), 373-384.
- Walker, L. J. (2004). Progress and prospects in the psychology of moral development. *Merrill-Palmer Quarterly*, 50(4), 546-557.
- Walker, L. J. (2006, September). *Moral personality exemplified. Symposium on Personality and Moral Character, Notre Dame, IN.*
- Walker, L. J. (2014). Prosocial exemplarity in adolescence and adulthood. In L. M. Padila-Walker & G. Carlo (Eds.), *Prosocial development: A multidimensional approach* (pp. 433-453). New York, NY: Oxford University Press.
- Walker, L. J., & Frimer, J. A. (2007). Moral personality of brave and caring exemplars. *Journal of Personality and Social Psychology*, 93(5), 845-860.
- Walker, L. J., & Frimer, J. A. (2008). Being good for goodness' sake: Transcendence in the lives of moral heroes. In F. Oser & W. Veugelers (Eds.), *Getting involved: Global citizenship development and sources of moral values* (pp. 309-326). Rotterdam, The Netherlands: Sense Publishers.
- Walker, L. J., & Frimer, J. A. (2009). Reconciling the self and morality: An empirical model of moral centrality development. *Developmental Psychology*, 45(6), 1669-1681.
- Walker, L. J., Frimer, J. A., & Dunlop, W. L. (2010). Varieties of moral personality: Beyond the banality of heroism. *Journal of Personality*, 78(3), 907-942.
- Walker, L. J., & Henning, K. H. (2004). Differing conceptions of moral exemplarity: Just, brave, and caring. *Journal of Personality and Social Psychology*, 86(4), 629-647.

- Walker, L. J., & Pitts, R. C. (1998). Naturalistic conceptions of moral maturity. *Developmental Psychology, 34*(3), 403-419.
- Walker, L. J., & Reimer, K. S. (2006). The relationship between moral and spiritual development. In E. C. Roehlkepartain, P. E. King, L. Wagener & P. L. Benson (Eds.), *The handbook of spiritual development in childhood and adolescence* (pp. 224-238). Thousand Oaks, CA: Sage.
- Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220.
- Weaver, G. R., & Agle, B. R. (2002). Religiosity and ethical behaviors in organizations: A symbolic interactionist perspective. *Academy of Management Review, 27*(1), 77-97.
- Webb, N. M., Shavelson, R. J., & Haertel, E. H. (2007). Reliability coefficients and generalizability theory. In C. R. Rao & S. Sinharay (Eds.), *Handbook of Statistics, Volume 26: Psychometrics* (Vol. 26, pp. 81-121). Oxford, UK: Elsevier.
- Whittingham, M. J., Stephens, P. A., Bradbury, R. B., & Freckleton, R. P. (2006). Why do we still use stepwise modelling in ecology and behaviour? *Journal of Animal Ecology, 75*(5), 1182-1189.
- Wildt, A. R., & Mazis, M. B. (1978). Determinants of scale response: Label versus position. *Journal of Marketing Research, 15*(2), 261-267.
- Williams, K. R. (2009). The noncommissioned officer as moral exemplar. *Military Review* Retrieved October 28, 2013, September-October, from [http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview\\_20091031\\_art017.pdf](http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20091031_art017.pdf)

- Williams, O. F., & Murphy, P. E. (1990). The ethics of virtue: A moral theory of marketing. *Journal of Macromarketing*, 10(2), 19-29.
- Wood, M. (2005). The fallacy of misplaced leadership. *Journal of Management Studies*, 42(6), 1101-1121.
- Woodward, B. S. (2007). Growth and training impact in IT: A measure of ethical reasoning. *Issues in Information Systems*, 8(2), 220-224.
- Woodward, B. S., & Ashby, S. (2006). Measuring growth and impact: Ethical reasoning in the information systems technology field. *Issues in Information Systems*, 7(1), 3-7.
- Woodward, B. S., Davis, D. C., & Hodis, F. A. (2007). The relationship between ethical decision making and ethical reasoning in information technology students. *Journal of Information Systems Education*, 18(2), 193-202.
- Wynd, C. A., Schmidt, B., & Schaefer, M. A. (2003). Two quantitative approaches for estimating content validity. *Western Journal of Nursing Research*, 25(5), 508-518.
- Xu, Y., Iran-Nejad, A., & Thoma, S. J. (2007). Administering defining issues test online: Do response modes matter? *Journal of Interactive Online Learning*, 6(1), 10-27.
- Yaghmaie, F. (2003). Content validity and its estimation. *Journal of Medical Education*, 3(1), 25-27.
- You, D., Maeda, Y., & Bebeau, M. J. (2011). Gender differences in moral sensitivity: A meta-analysis. *Ethics & Behavior*, 21(4), 263-282.
- Zerbe, W. J., & Paulhus, D. L. (1987). Socially desirable responding in organizational behavior: A reconception. *The Academy of Management Review*, 12(2), 250-264.